



## **Federal Supply Service**

### **Authorized Federal Supply Schedule Price List**

On line access to contract ordering information, terms and conditions, up to date pricing, and the option to create an electronic delivery order are available through GSA Advantage!®, a menu driven database system. The INTERNET address GSA Advantage!® is: GSAAvantage.gov.

**SCHEDULE TITLE:** MULTIPLE AWARD SCHEDULE (MAS)

For more information on ordering from Federal Supply Schedules go to the GSA Schedules page at GSA.gov.

SEALING TECHNOLOGIES INC  
7134 COLUMBIA GATEWAY DR, STE 160  
COLUMBIA, MD 21046-3373  
Phone: 443-537-9726  
Website: <https://www.sealingtech.com/>  
Point of Contact: Daniel Zick, CFO

---

***Contract Number: GS-35F-056CA***  
***Contract Period: November 3, 2014 - November 2, 2024***  
***Business Size: Veteran Owned Small business***  
***Solicitation 47QSMD20R0001***  
***Modification 50 (effective December 11, 2020)***

Customer Information

**1a. TABLE OF AWARDED SPECIAL ITEM NUMBERS (SINs)**

SIN 511210 – Software Licenses  
SIN 33411 – Purchasing of new electronic equipment  
SIN 54151HACS – Highly Adaptive Cybersecurity Services (HACS)  
SIN 54151S – Information Technology Professional Services  
SIN 611420 – Information Technology Training  
SIN ANCILLARY – Ancillary Supplies and Services  
SIN OLM – Order-Level Materials (OLM)

**1b. Identification of the lowest priced model number and lowest unit price for that model for each special item number awarded in the contract. This price is the Government price based on a unit of one, exclusive of any quantity/dollar volume, prompt payment, or any other concession affecting price. Those contracts that have unit prices based on the geographic location of the customer, should show the range of the lowest price, and cite the areas to which the prices apply. See Price List**

**1c. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles, experience, functional responsibility and education for those types of employees or subcontractors who will perform services shall be provided. See Price List**

**2. Maximum order.** \$250,000 (611420, ANCILLARY, OLM); \$500,000 (all other SINs)

**3. Minimum order.** \$100.00

**4. Geographic coverage (delivery area).** Domestic Delivery. Domestic delivery is delivery within the 48 contiguous states, Alaska, Hawaii, Puerto Rico, Washington, DC, and U.S. Territories. Domestic delivery also includes a port or consolidation point, within the aforementioned area, for orders received from overseas activities.

**5. Point(s) of production.** Columbia, Howard County, MD

**6. Discount from list prices or statement of net price.** Prices shown are net; discounts have been deducted.

**7. Quantity discounts.** 2% for any order over \$500,000 (services only)

# SEALING TECH

Taking Cyber Security Seriously

**8. Prompt payment terms.** Net 30. Information for Ordering Offices: Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions.

**9. Foreign items.** None

**10a. Time of delivery.** SIN 511210 (30 Days ARO); SIN 33411 (90 Days ARO)

**10b. Expedited Delivery.** Contact Contractor

**10c. Overnight and 2 day delivery.** Contact Contractor

**10d. Urgent Requirements.** Contact Contractor

**11. F.O.B. point(s).** Destination

**12a Ordering address.**

Sealing Technologies, Inc.  
7134 Columbia Gateway Drive, Suite 160  
Columbia, MD 21046  
(443) 542-0040

**12b. Ordering procedures.** For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPA's) are found in Federal Acquisition Regulation (FAR) 8.405-3.

**13. Payment address.** Same as ordering address

**14. Warranty provision.** Standard Commercial Warranty

**15. Export packing charges.** Not Applicable

**16. Terms and conditions of rental, maintenance, and repair.** Not Applicable

**17. Terms and conditions of installation.** Not Applicable

**18a. Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices.** Not Applicable

**18b. Terms and conditions for any other services.** Not Applicable

**19. List of service and distribution points.** Not Applicable

**20. List of participating dealers.** Not Applicable

**21. Preventive maintenance.** Not Applicable

**22a. Special attributes such as environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants).** Not Applicable

**22b. If applicable, indicate that Section 508 compliance information is available on Electronic and Information Technology (EIT) supplies and services and show where full details can be found (e.g. contractor's website or other location.) The EIT standards can be found at: [www.Section508.gov/](http://www.Section508.gov/).** Not Applicable

**23. Data Universal Number System (DUNS) number.** 078491625

**24. Notification regarding registration in System for Award Management (SAM) database.** Registered

## Labor Category Descriptions

Labor Category	Description	Years of Experience	Education and Substitution
1. Business Process Engineer I	Applies process improvement and reengineering methodologies and principles to conduct process modernization projects. Performs activity and data modeling, develops modern business methods, identifies best practices and creates and assesses performance measurements. Provides group facilitation, interviewing, and training and provides additional forms of knowledge transfer.	2 years of relevant experience	Bachelor's degree in a related field
2. Business Process Engineer II	Applies process improvement and reengineering methodologies and principles to conduct process modernization projects. Performs activity and data modeling, develops modern business methods, identifies best practices and creates and assesses performance measurements. Provides group facilitation, interviewing, and training and provides additional forms of knowledge transfer.	4 years of relevant experience	Bachelor's degree in a related field
3. Business Process Engineer III	Applies advanced process improvement and reengineering methodologies and principles to conduct process modernization projects. Performs activity and data modeling, develops modern business methods, identifies best practices and creates and assesses performance measurements. Provides group facilitation, interviewing, and training and provides additional forms of knowledge transfer.	6 years of relevant experience	Bachelor's degree in a related field
4. Computer Security Systems Specialist I	Under specific direction, analyzes user needs and current security regulations and guidelines to determine IA functional requirements. Provides Information Security Controls and guidelines to nodes and network management systems. Maintains network/system access and password controls. Collates and analyzes audit trail data. Reviews security threats and determines/implements effective countermeasures IAW established policies/regulations/directives. Analyzes network or system changes/reconfigurations for security impacts (performs risk analysis/assessment). Documents security measures policies.	1 year of relevant experience	Associates degree in a related field or industry standard security certification
5. Computer Security Systems Specialist II	Under general supervision, analyzes and defines security requirements. Provides Information Security Controls and guidelines to nodes and network management systems. Maintains network/system access and password controls. Collates and analyzes audit trail data. Reviews security threats and determines/implements effective countermeasures IAW established policies/regulations/directives. Analyzes network or system changes/reconfigurations for security impacts (performs risk analysis/assessment). Documents security measures policies. Knowledgeable of Security/IA products such as PKI, VPN, firewalls, and intrusion detection systems. Analyzes and recommends resolution of security/IA problems on the basis of	3 years of relevant experience	Bachelor's degree in a related field or industry standard security certification

	knowledge of the major IA products and services, an understanding of their limitations, and knowledge of the IA disciplines.		
6. Computer Security Systems Specialist III	Analyzes and defines security requirements for complex engineering issues. Designs, develops, engineers, and implements solutions to system architectural requirements. Gathers and organizes technical information about an organization's mission goals and needs, existing security products, and ongoing programs. Performs risk analyses and assessments. Provides daily supervision and direction to staff. Provides technical support for secure software development and integration tasks, including reviewing work products for correctness and adhering to the design concept and to user standards. Knowledgeable of Security/Information Assurance (IA) products such as PKI, VPN, firewalls, and intrusion detection systems. Analyzes and recommends resolution of security/IA problems on the basis of knowledge of the major IA products and services, an understanding of their limitations, and knowledge of the IA disciplines. Provides daily supervision and direction to staff when leading a team.	6 years of relevant experience	Bachelor's degree in a related field or industry standard security certification
7. Consultant I	Working directly with customer engineers, applies focused expertise as a specialist in the planning, deployment, operation and/or enhancement of advanced information systems and networks. Plans, coordinates and performs complex assignments under minimal supervision. Compares network or system architecture alternatives for interfacing switching, bandwidth management and network operations equipment and functions. Establishes details for implementing new means of achieving and provisioning process/system requirements. Translates process requirements into action plans. Addresses technical and procedural issues raised by customers, as related to best industry practices.	3 years of relevant experience	Associate's Degree in a related field
8. Consultant II	Works directly with customer management in applying intermediate principles, theories and concepts to a wide range of work in the areas of planning, deployment, operation and/or enhancement of advanced telecommunications and information technology systems networks. Works on complex problems and provides solutions that are innovative and often involve reevaluation of established theories and practices, leading to new and creative solutions to problems. Defines network architecture alternative for interfacing transmission, switching, bandwidth management and network operations equipment and functions. Develops new means of achieving provisioning and billing process/system requirements. Resolves technical and procedural issues raised by customers, as related to best industry practices. Provides practical guidance on deployment planning for new network/service rollouts and for transition from existing networks. Develops alternative technical solutions in situations	5 years of relevant experience	Bachelor's Degree in a related field

	where customer has conflicting advice. Provides functional guidance, supervision, technical support, training and quality assurance/quality control to Associate personnel.		
9. Consultant III	Working directly with customer management, applies advanced principles, theories and concepts that contribute to sustained technical excellence of solutions. Manages the technical output of other Consultants, or works independently on unstructured problems and issues involving multivariate factors based on factual or hypothetical data solution may be innovative or original in nature. Defines leading edge concepts for planning, deployment, operation and/or enhancement of advanced information systems and networks. Guides others on solution paths for resolving problems. Assesses technical and cost impacts. Establishes technical recommendations in situations where customer has conflicting advice. Provides functional guidance, supervision, technical support, training and quality assurance/quality control to Associate and Intermediate personnel. Supports senior staff as required and ensures customer requirements and project milestones are met.	7 years of relevant experience	Bachelor's Degree in a related field
10. Functional Analyst I	Analyzes user needs to determine functional requirements. Performs functional allocation to identify required tasks and their interrelationships. Identifies resources required for each task. Provides functional guidance, supervision, technical support, training, and quality assurance/quality control to more junior personnel.	2 years of relevant experience	High School Diploma
11. Functional Analyst II	Analyzes user needs to determine functional and cross-functional requirements. Performs functional allocation to identify required tasks and their interrelationships. Identifies resources required for each task. Provides daily supervision and direction to support staff.	3 years of relevant experience	Associate's Degree in a related field
12. Information Assurance Specialist I	Under specific guidance, performs technical support focused on the development, operation, management, and enforcement of security capabilities for systems and networks. Technical support is concentrated on the protection and defense of information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for their restoration by incorporating protection, detection, and reaction capabilities.	2 years of relevant experience	At least 60 semester hours of education in a related field and a technical certification listed in DoD 8570.01 IAT level I or DoD 8570.01 IAM level I requirements
13. Information Assurance Specialist II	Under general supervision, performs technical support focused on the development, operation, management, and enforcement of security capabilities for systems and networks. Technical support is concentrated on the protection and defense of	2-5 years of relevant experience	At least 60 semester hours of education in a related field and a technical

	information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.		certification listed in DoD 8570.01 IAT level II or DoD 8570.01 IAM level II requirements
14. Information Assurance Specialist III	Works independently or manages a team of security engineers to apply advanced security knowledge to programs. Performs technical support focused on the development, operation, management, and enforcement of security capabilities for systems and networks. Technical support is concentrated on the protection and defense of information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for their restoration by incorporating protection, detection, and reaction capabilities.	6 or more years of relevant experience	Bachelor's degree in a related field and a technical certification listed in DoD 8570.01 IAT level II or DoD 8570.01 IAM level II requirements
15. Information Systems Security Specialist I	Provides Information Security Controls and guidelines. Maintains network/system access and password controls. Collates and analyzes audit trail data. Reviews security threats and determines/implements effective countermeasures IAW established policies/regulations/directives. Analyzes network or system changes/reconfigurations for security impacts (performs risk analysis/assessment). Documents security measures/policies. Performs functions as required in support of NIST SP 800-53, the DoD 8500 series, and other applicable Government, network, system, or customer-specific security requirements.	3 years of relevant experience	Associates degree in a related field or industry standard security certification
16. Information Systems Security Specialist II	Manages Information Systems Security personnel and provides oversight to security program(s) projects. Assesses configuration changes for security impacts; assists in the development of alternate courses of action or implementation of resultant measures. Performs system administration functions to include, but not limited to, documenting the security architecture. Develops user security guidelines and SOPS. Performs functions as required in support of NIST SP 800-53, the DoD 8500 series, and other applicable Government, network, system, or customerspecific security requirements. As required, performs those duties described in Information System Security Specialist I.	5 years of relevant experience	Bachelor's degree in a related field or industry standard security certification
17. Information Technology Consultant I	Experience with several ADP architectures and platforms in an integrated environment. Stays current with advances in information technology. Assists in the analysis of current and projected service maintenance personnel and facility requirements. Designs interfaces to allow incompatible equipment to function as a unified system.	3 years of relevant experience	Bachelor's degree in a related field

18. Information Technology Consultant II	Leads major portions of large or medium projects and leads small projects autonomously. Gathers facts through research, interviewing, surveys, etc. Analyzes the client's business, draws conclusions, prepares final reports and gives presentations. Uses in-depth consultative skills and business knowledge to practice business objectives and processes. Manages and implements large, complex information technology systems. Advises senior executives on effective utilization of information technology systems and reengineering to meet business objectives. Identifies user requirements and describes services available or refers inquiries to other staff within installation. Provides technical support of a limited scope to users and assists them in defining and solving computing problems within well-defined areas of responsibility. Assists in preparing documentation of supported products for other staff members and users. Assists in preparing user training materials and conduct training sessions as assigned. Performs programming tasks of limited scope to assist users.	4 years of relevant experience	Bachelor's degree in a related field
19. Information Technology Consultant III	Manages the project work as defined by the client contract. Leads medium to large complex projects and major phases of very large projects. Manages the fact-finding, analysis, and development of hypothesis/conclusions, production of final reports, and delivery of presentations. Ensures that the project delivers to client expectations on time and to budget.	6 years of relevant experience	Bachelor's degree in a related field
20. Information Technology Consultant IV	Manages and implements large, complex information technology systems. Experienced in advising senior executives on effective utilization of information technology systems and reengineering to meet business objectives. Identifies user requirements and describes services available or refers inquiries to other staff within installation. Provides technical support of a limited scope to users and assists them in defining and solving computing problems within well-defined areas of responsibility. Assists in preparing documentation of supported products for other staff members and users. Assists in preparing user training materials and conducts training sessions as assigned. Performs programming tasks of limited scope to assist users.	6 years of relevant experience	Master's degree in a related field

<p>21. Information Technology Consultant V</p>	<p>Serves as a Management Information System (MIS) manager. Designs, develops and manages implementation of risk assessment and business contingency planning framework, methodology, and tools to ensure business continuity of operations across a large, multi-division, decentralized organization. Supports multi-language, multi-platform and multioperating system operations and utilizes electronic commerce and Electronic Data Interchange (EDI) applications. Recognizes and recommends new or emerging technology or software to satisfy functional requirements and processes. Provides highly technical and/or specialized guidance concerning automation solutions to complex information processing problems related to the subject field. Provides customer support using enterprise solutions software to integrate business areas consistent with today's technology in order to operate in an open systems environment and client service architecture. Analyzes data processing requirements to plan EDP systems to provide system capabilities required for projected workloads. Plans layout and installation of new systems or modification of existing systems. May set up and control analog or hybrid computer systems to solve scientific and engineering problems. Knowledgeable in Oracle, Windows NT, network administration, project management and Unix and Cobol programming. Internet Development/Integration. Develops applications that take advantage of Internet protocols and platforms. Internet developers extend beyond traditional software development disciplines to demonstrate advanced graphical design abilities, familiarity with new media formats, and solid understanding of Internet communications protocols and services. Deploys new applications that utilize Internet standards to enable wide access from the diverse client types found throughout the public Internet.</p>	<p>8 years of relevant experience</p>	<p>Master's degree in a related field</p>
--	--	---------------------------------------	---

<p>22. Information Technology Consultant VI</p>	<p>Senior consultant to top level management. Viewed as the expert in discipline or related area of expertise, exhibiting an exceptional degree of ingenuity, creativity, and resourcefulness. Managerial/leadership experience required. Typically serves as the prime spokesperson to the customer. Performs technical planning, system integration, verification and validation, cost and risk, and supportability and effectiveness analyses for total systems. Analyses are performed at all levels of total system product to include: hardware/software, concept, design, fabrication, test, installation, operation, maintenance, and disposal. Performs duties such as site surveys, system evaluation, system analysis, architecture, and infrastructure assessment. Ensures the logical and systematic conversion of customer or product requirements into total systems solutions that acknowledge technical, schedule, and cost constraints. Applies and/or develops advanced technologies, scientific principles, theories, and concepts. Often acts independently to resolve issues associated with the development and implementation of operational programs. Plans R&amp;D programs and recommends technological application programs to accomplish long-range objectives.</p>	<p>10 years of relevant experience</p>	<p>Master's degree in a related field</p>
<p>23. Information/Computer/Telecommunications Specialist I</p>	<p>With specific guidance, performs technical assignments in the general areas of Command and Control Systems, Automated Information Systems, and National Security Systems, applying broad technical knowledge in one or more areas on specific systems or applications. Work requires knowledge of customary approaches, techniques, and requirements appropriate to the assigned program, including legacy systems, and latest trends in related technologies. Requires specialized experience in evaluating, analyzing, operating, maintaining, managing, or improving Command and Control Systems, Automated Information Systems, and National Security System's performance, procedures, and requirements</p>	<p>Up to 3 years of directly related experience</p>	<p>High School Diploma and a technical certification directly related to this labor category</p>
<p>24. Information Computer Telecommunications Specialist II</p>	<p>With general guidance, performs technical assignments in the general areas of Command and Control Systems, Automated Information Systems, and National Security Systems, applying broad technical knowledge in one or more areas on specific systems or applications. Work requires knowledge of customary approaches, techniques, and requirements appropriate to the assigned program, including legacy systems, and latest trends in related technologies. Requires specialized experience in evaluating, analyzing, operating, maintaining, managing, or improving Command and Control Systems, Automated Information Systems, and National Security System's performance, procedures, and requirements.</p>	<p>At least 3 years of directly related experience</p>	<p>High School Diploma and at least one intermediate technical certification directly related to this labor category</p>

<p>25. Information/Computer/Telecommunications Specialist III</p>	<p>Works independently or manages a team of engineers that performs technical assignments in the general areas of Command and Control Systems, Automated Information Systems, and National Security Systems, applying broad technical knowledge in one or more areas on specific systems or applications. Work requires knowledge of customary approaches, techniques, and requirements appropriate to the assigned program, including legacy systems, and latest trends in related technologies. Requires specialized experience in evaluating, analyzing, operating, maintaining, managing, or improving Command and Control Systems, Automated Information Systems, and National Security System's performance, procedures, and requirements.</p>	<p>At least 7 years of relevant experience</p>	<p>High School Diploma and at least one advanced technical certification directly related to this labor category</p>
<p>26. Network Design Engineer I</p>	<p>Provides basic engineering direction to the design of network systems. Develops multiple alternate designs at each development level, and trade-off results that trigger iteration of the design process. Designs complex networks that typically link numerous computing platforms, operating systems, and network topologies across local areas. Responsible for the implementation of engineering processes that provide for timely and appropriate integration of all engineering disciplines to ensure a network system design that meets all requirements. Identifies problems and risk areas and mitigates their impact. Performs technical design reviews.</p>	<p>1 year of relevant experience</p>	<p>Bachelor's Degree in a related field</p>
<p>27. Network Design Engineer II</p>	<p>Provides intermediate level engineering direction to the design of network systems. Develops and implements strategy for generating multiple alternate designs at each development level, and trade-off results which trigger iteration of the design process. Designs and implements highly complex networks that typically link numerous computing platforms, operating systems, and network topologies across widely dispersed geographical areas. Responsible for the implementation of engineering processes that provide for timely and appropriate integration of all engineering disciplines to ensure a network system design that meets all requirements. Identifies problems and risk areas and mitigates their impact. Performs technical design reviews. Provides functional guidance, supervision, technical support, training and quality assurance/quality control to Associate personnel.</p>	<p>3 years of relevant experience</p>	<p>Bachelor's Degree in a related field</p>

28. Network Design Engineer III	Provides leadership and engineering direction to the design of network systems. Develops and implements strategy for generating multiple alternate designs at each development level, and trade-off results which trigger iteration of the design process. Designs and implements highly complex networks that typically link numerous computing platforms, operating systems, and network topologies across widely dispersed geographical areas. Responsible for the implementation of engineering processes that provide for timely and appropriate integration of all engineering disciplines to ensure a network system design that meets all requirements. Identifies problems and risk areas and mitigates their impact. Performs technical design reviews. Provides functional guidance, supervision, technical support, training, and quality assurance/quality control to Associate and Intermediate personnel. Supports senior staff as required and ensures customer requirements and project milestones are met.	7 years of relevant experience	Bachelor's Degree in a related field
29. Network Systems Engineer I	Provides technical engineering assistance in the implementation phase of Local Area Networking practices. Monitors network topologies; develops and evaluates alternative utilization or configuration options. Monitors and reports network performance analysis. Assists in network testing, technology insertion, and developmental software applications and evaluation/testing as required.	2 years of relevant experience	Associate's Degree in a related field
30. Network Systems Engineer II	Provides technical engineering assistance to the design and implementation phases of network development, operation, and management. Monitors network topologies; develops and evaluates alternative utilization or configuration options. Conducts performance and trend analysis. Develops processes and programs to enhance network performance and reliability. Conducts network testing, technology insertion, and developmental software application testing as required. Provides functional guidance, supervision, technical support, training, and quality assurance/quality control to Associate personnel.	4 years of relevant experience	Associate's Degree in a related field
31. Network Systems Engineer III	Provides senior level technical engineering assistance to all phases of network development, operation, and management. Monitors network topologies; develops and evaluates alternative utilization or configuration options. Conducts network performance and trend analysis. Develops processes and programs to enhance network performance and reliability. Conducts network testing, supervises technology insertion, and evaluates developmental software applications. Provides functional guidance, supervision, technical support, training, and quality assurance/quality control to Associate and Intermediate personnel. Supports senior staff as required and ensures customer requirements and project milestones are met.	6 years of relevant experience	Bachelor's Degree in a related field

32. Operations Manager	Manages computer services contract related operations. Ensures production schedules are met. Ensures computer system resources are used effectively. Coordinates the resolution of production related problems. Ensures proper relationships are established between customers, teaming partners, and vendors to facilitate the delivery of information technology services. Provides users with computer output and supervises staff operations.	5 years of relevant experience	Bachelor's degree in a related field, PMP certification
33. Program Administration Specialist	Assists in the preparation of management plans and reports. Coordinates schedules to facilitate completion of proposals, contract deliverables, task order review, briefings/presentations and IPR preparation. Performs analysis, development, and review of program administrative operating procedures.	1 year of relevant experience	Associates Degree in a related field
34. Program Manager	Serves as the contractor's single contract manager and shall be the contractor's authorized interface with the Government Contracting Officer (CO), Government management personnel and customer agency representatives. Responsible for formulating and enforcing work standards, assigning contractor schedules, reviewing work discrepancies, supervising contractor personnel and communicating policies, purposes, and goals of the organization to subordinates.	6 years of relevant experience	Bachelor's degree in a related field, PMP certification
35. Project Manager	Manager to include but not limited to: all financial management and administrative activities, such as budgeting, manpower and resource planning and financial reporting. Performs complex evaluations of existing procedures, processes, techniques, models, and/or systems related to management problems or contractual issues that require reports and recommends solutions. Prepares charts, tables, graphs, and diagrams to assist in analyzing problems. Provides supervision, training and direction to staff.	3 years of relevant experience	Associate's degree in a related field, PMP
36. Quality Assurance Analyst	Evaluates all components associated with hardware, software, network, systems, or communications and associated documentation. Performs basic quality control checks as directed. Participates in formal and informal reviews to evaluate adherence to requirements and specifications and determines quality.	1 year of relevant experience	Associate's Degree in a related field
37. Quality Assurance Manager	Establishes and maintains a process for evaluating all components associated with hardware, software, network, systems, or communications and associated documentation. Determines the resources required for quality control. Maintains the level of quality throughout the life cycle. Conducts formal and informal reviews at pre-determined points throughout the life cycle. Provides daily supervision and direction to support staff.	3 years of relevant experience	Bachelor's Degree in a related field

<p>38. Software Developer I</p>	<p>With general guidance, provides technical expertise, including performing software systems programming and development. Implements architectures using a variety of developmental tools and languages (e.g. Java, .NET, SQL, Python, etc.). Ensures the developed applications are compatible and in compliance with the standards for open systems and Federal architectures. Determines and identifies high level functional and technical requirements based on interactions with the user community and knowledge of the enterprise architecture. Identifies, assesses, and presents options for meeting the functional and technical requirements including hardware and software updates or upgrades. Develops software design documents and technology white papers. Responsible for developing high level system design diagrams and for program design, coding, testing, debugging and documentation.</p>	<p>1 year of relevant experience</p>	<p>Bachelor's degree in a related field</p>
<p>39. Software Developer II</p>	<p>With minimum guidance, provides intermediate level technical expertise, including performing software systems programming and development. Implements architectures using a variety of developmental tools and languages (e.g. Java, .NET, SQL, Python, etc.). Ensures these systems are compatible and in compliance with the standards for open systems and DoD/Federal architectures. Determines and identifies high level functional and technical requirements based on interactions with the user community and knowledge of the enterprise architecture. Identifies, assesses, and presents options for meeting the functional and technical requirements including hardware and software updates or upgrades. Formulates and defines specifications for operating system applications or modifies and maintains existing applications using engineering releases and utilities from the manufacturer. Creates detailed design specifications for use by software development staff members. Interacts with project management to plan project schedules and technical direction. Develops software design documents and technology white papers. Instrumental in selection of development tools. Responsible for developing high level system design diagrams and for program design, coding, testing, debugging and documentation.</p>	<p>3 years of relevant experience</p>	<p>Bachelor's degree in a related field</p>
<p>40. Software Developer III</p>	<p>With no guidance, provides expert level technical expertise, including performing software systems programming and development. Designs, Implements, and Reviews architectures using a variety of developmental tools and languages (e.g. Java, .NET, SQL, Python, etc.). Designs architectures to include the software, hardware, and communications to support the total requirements as well as provide for present and future cross functional requirements and interfaces. Determines and identifies high level functional and technical requirements based on interactions with the user community and knowledge of the enterprise architecture. Formulates and defines specifications for</p>	<p>5 years of relevant experience</p>	<p>Master's degree in a related field</p>

	<p>operating system applications or modifies and maintains existing applications using engineering releases and utilities from the manufacturer. Creates detailed design specifications for use by software development staff members. Interacts with project management to plan project schedules and technical direction. Develops software design documents and technology white papers. Instrumental in selection of development tools. Responsible for developing high level system design diagrams and for program design, coding, testing, debugging and documentation. Instructs, directs, and checks the work of other task personnel. Responsible for quality assurance review and the evaluation of existing and new software products.</p>		
41. Subject Matter Expert I	<p>Under broad direction, provides support, analysis, and research into complex problems and processes relating to the subject matter. Serves as technical advisor on high-level project teams providing technical direction, interpretation, and alternatives. Thinks independently and demonstrates superior written and oral communications skills. Possesses a complete understanding and wide experience in the application of technical principles, theories, and concepts in the field. Provides technical solutions to a wide range of difficult problems. Solutions are imaginative, thorough, practicable, and consistent with organizational objectives. Independently determines and develops approach to solutions. Contributes to the completion of specific programs and projects. Possesses expertise in a particular area of Information Technology (e.g., Information Systems Architecture, Telecommunications Systems Design, Architecture, Implementation, Information Systems Integration, Software Development Methodologies, Security Engineering, Communications and Network Systems Management), or a specific functional area (e.g., finance, logistics, and operations research).</p>	4 years of relevant experience	Bachelor's Degree in a related field

<p>42. Subject Matter Expert II</p>	<p>With minimal direction, provides Intermediate level support, analysis, and research into exceptionally complex problems and processes relating to the subject matter. Serves as technical expert on executive-level project teams providing technical direction, interpretation and alternatives. Thinks independently and demonstrates exceptional written and oral communications skills. Applies extensive technical expertise 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. Exercises considerable latitude in determining technical objectives of assignment. Possesses expertise in a particular area of Information Technology (e.g., Information Systems Architecture, Telecommunications Systems Design, Architecture, Implementation, Information Systems Integration, Software Development Methodologies, Security Engineering, Communications and Network Systems Management), or a specific functional area (e.g., finance, logistics, and operations research)</p>	<p>6 years of relevant experience</p>	<p>Bachelor's degree in a related field</p>
<p>43. Subject Matter Expert III</p>	<p>Provides expert support, analysis, and research into exceptionally complex problems and processes relating to the subject matter. Serves as technical expert on executive-level project teams providing technical direction, interpretation and alternatives. Thinks independently and demonstrates exceptional written and oral communications skills. Applies advanced technical principles, theories, and concepts. Contributes to the development of new principles and concepts. Works on unusually complex technical problems and provides solutions which are highly innovative. Works under consultative direction toward predetermined long-range goals and objectives. Assignments are often self-initiated. Determines and pursues courses of action necessary to obtain desired results. Develops advanced technological ideas and guides their development into a final product. Possesses expertise in a particular area of Information Technology (e.g., Information Systems Architecture, Telecommunications Systems Design, Architecture, Implementation, Information Systems Integration, Software Development Methodologies, Security Engineering, Communications and Network Systems Management), or a specific functional area (e.g., finance, logistics, and operations research).</p>	<p>4 years of relevant experience</p>	<p>Master's degree in a related field</p>

<p>44. Subject Matter Expert IV</p>	<p>Provides architecture and engineering SME support across multiple enterprise level initiatives. Determines and identifies high-level functional and technical requirements based on interactions with the user community and knowledge of the existing enterprise architecture. Designs enterprise architectures to include the software, hardware and communications to support the enterprise requirements as well as provide for present and future cross-functional requirements and interfaces. Identifies, assesses, and presents options for meeting the functional and technical requirements including hardware and software updates or upgrades. Develops high-level system design diagrams. Ensures systems are compatible and in compliance with the standards for open systems architectures, the Open Systems Interconnection (OSI) and International Standards Organization (ISO) reference models, and profiles of standards. Ensures compliance with standards and directives. Evaluates problems of work flows, organization and planning and develops appropriate corrective action. Evaluates and recommends new technologies.</p>	<p>6 years of relevant experience</p>	<p>Master's degree in a related field</p>
<p>45. Systems Administrator I</p>	<p>With broad direction, performs routine and recurring assignments, identifies and resolves issues and problems, provides information and assistance to customers, ensures the application of appropriate security measures are in place. Has knowledge of, and skill in applying operating systems installation and configuration procedures, ability to install, configure, and maintain operating systems components; install updates and temporary fixes to existing application programs. Has knowledge of, and skill in applying systems administration methods and procedures, software distribution tools, data recovery tools and techniques. Monitors and troubleshoots systems availability, recover data in event of hardware or software failure. Supervises and manages the daily activities of configuration and operation of business systems which may be mainframe, mini, or client/server based. Optimizes system operation and resource utilization and performs system capacity analysis and planning. Provides assistance to users in accessing and using business systems.</p>	<p>2 years of relevant experience</p>	<p>High School Diploma and at least 1 System Administrative related technical certification</p>

<p>46. Systems Administrator II</p>	<p>With broad direction, performs routine and recurring assignments, identifies and resolves issues and problems, provides information and assistance to customers, ensures the application of appropriate security measures are in place. Has knowledge of, and skill in applying operating systems installation and configuration procedures, ability to install, configure, and maintain operating systems components; install updates and temporary fixes to existing application programs. Has knowledge of, and skill in applying systems administration methods and procedures, software distribution tools, data recovery tools and techniques. Monitors and troubleshoots systems availability, recover data in event of hardware or software failure. Supervises and manages the daily activities of configuration and operation of business systems which may be mainframe, mini, or client/server based. Optimizes system operation and resource utilization and performs system capacity analysis and planning. Provides assistance to users in accessing and using business systems.</p>	<p>3 years of relevant experience</p>	<p>Associates degree and at least one System Administrative related technical certification</p>
<p>47. Systems Administrator III</p>	<p>With little or no direction, organizes and directs the configuration and operation of information management systems. Responsible for directing the work of other system administrators to provide the day-to-day system administration to include system and resource optimization, and user assistance. Conducts capacity and performance analysis and provides system configuration change and upgrade recommendations. Increases system administrator efficiency and accuracy via the use of automated tools and scripts, develops system administrator procedures, and conducts system administrator training and skills assessment.</p>	<p>4 years of relevant experience</p>	<p>Bachelor's degree in a related field</p>

<p>48. Systems Architect III</p>	<p>With minimal direction, establishes system information requirements using analysis of the information engineer(s) in the development of enterprise-wide or large-scale information systems. Determines and identifies high level functional and technical requirements based on interactions with the user community and knowledge of the enterprise architecture. Designs architecture to include the software, hardware and communications to support the total requirements as well as provide for present and future cross-functional requirements and interfaces. Identifies, assesses, and presents options for meeting the functional and technical requirements including hardware and software updates or upgrades. Responsible for developing high level system design diagrams. Ensures these systems are compatible and in compliance with all applicable standards. Ensures that the common operating environment is compliant. Evaluates analytically and systematically problems of work flows, organization and planning and develops appropriate corrective action.</p>	<p>4 years of relevant experience</p>	<p>Bachelor's Degree in a related field</p>
<p>49. Systems Architect IV</p>	<p>With little or no direction, establishes system information requirements using analysis of the information engineer(s) in the development of enterprise-wide or large-scale information systems. Determines and identifies high level functional and technical requirements based on interactions with the user community and knowledge of the enterprise architecture. Designs architecture to include the software, hardware and communications to support the total requirements as well as provide for present and future cross-functional requirements and interfaces. Identifies, assesses, and presents options for meeting the functional and technical requirements including hardware and software updates or upgrades. Responsible for developing high level system design diagrams. Ensures these systems are compatible and in compliance with all applicable standards. Ensures that the common operating environment is compliant. Evaluates analytically and systematically problems of work flows, organization and planning and develops appropriate corrective action. Provides daily supervision and direction to engineering staff.</p>	<p>6 years of relevant experience</p>	<p>Bachelor's Degree in a related field</p>
<p>50. Systems Engineer I</p>	<p>With broad direction, evaluates and/or implements system architectures and design into functional processes. Works as a member of an engineering team to assess the feasibility of use cases, design user and system interfaces. Installs, updates, configures, and validates the functionality of custom applications. Implements the security controls and requirements for custom applications. Follows the direction and supervision of higher level system engineers.</p>	<p>At least 1 year of relevant experience</p>	<p>Associates degree in a related field</p>

51. Systems Engineer II	With some direction, evaluates and/or implements system architectures and design into functional processes. Works as a member of an engineering team to assess the feasibility of use cases, design user and system interfaces. Installs, updates, configures, and validates the functionality of custom applications. Implements the security controls and requirements for custom applications. Follows the direction and supervision of higher level system engineers.	At least 3 years of relevant experience	Bachelor's degree in a related field
52. Systems Engineer III	With minimal direction, evaluates and/or implements system architectures and design into functional processes. Works in a leadership role within an engineering team to assess the feasibility of use cases, design user and system interfaces. Installs, updates, configures, and validates the functionality of custom applications. Implements the security controls and requirements for custom applications. Provides direction and supervision to lower level engineers.	At least 6 years of relevant experience	Bachelor's degree in a related field
53. Task Order Manager	Serves as the project manager for a large, complex task order (or a group of task orders affecting the same common/standard/migration system) and shall assist the Program Manager in working with the Government Contracting Officer (CO), the task order level TMs, Government management personnel and customer agency representatives. Under the guidance of the Program Manager, responsible for the overall management of the specific task order(s) and ensuring that the technical solutions and schedules in the task order are implemented in a timely manner. Performs enterprise-wide horizontal integration planning and interfaces to other functional systems.	6 years of relevant experience	Bachelor's degree in a Management, Business, or Technical field, PMP certification
54. Technical Writer/ Editor II	Assists in collecting and organizing information required for preparation of user manuals, training materials, installation guides, proposals, and reports. Edit functional descriptions, system specifications, user manuals, special reports, or any other customer deliverables and documents. Assists in performing financial and administrative functions.	1 year of relevant experience	Associates degree in English or in a Computer or Engineering field
55. Technical Writer/ Editor III	Assists in collecting and organizing information required for preparation of user manuals, training materials, installation guides, proposals, and reports. Edits functional descriptions, system specifications, user manuals, special reports, or any other customer deliverables and documents. Assists in performing financial and administrative functions. Provides functional guidance, supervision, technical support, training, and quality assurance/quality control to Associate personnel.	3 years of relevant experience	Bachelor's degree in English or in a Computer or Engineering field

<p>56. PT- Computer Security Systems Specialist I</p>	<p>Under specific direction, analyzes user needs and current security regulations and guidelines to determine IA functional requirements. Provides Information Security Controls and guidelines to nodes and network management systems. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Coordinates with system and network owners to cooperatively review architectures and provide advisement on vulnerabilities with associated remediation recommendations. Maintains network/system access and password controls. Collates and analyzes audit trail data. Reviews security threats and determines/implements effective countermeasures IAW established policies/regulations/directives. Analyzes network or system changes/reconfigurations for security impacts (performs risk analysis/assessment). Documents security measures policies.</p>	<p>1 year</p>	<p>Associates degree in a related field or security certification (CCNA or CEH)</p>
<p>57. PT- Computer Security Systems Specialist II</p>	<p>Under general supervision, analyzes and defines security requirements. Provides Information Security Controls and guidelines to nodes and network management systems. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Coordinates with system and network owners to cooperatively review architectures and provide advisement on vulnerabilities with associated remediation recommendations. Maintains network/system access and password controls. Collates and analyzes audit trail data. Reviews security threats and determines/implements effective countermeasures IAW established policies/regulations/directives. Analyzes network or system changes/reconfigurations for security impacts (performs risk analysis/assessment). Documents security measures policies. Knowledgeable of Security/IA products such as PKI, VPN, firewalls, and intrusion detection systems. Analyzes and recommends resolution of security/IA problems on the basis of knowledge of the major IA products and services, an understanding of their limitations, and knowledge of the IA disciplines.</p>	<p>3 years</p>	<p>Bachelor's degree in a related field or security certification (CCNA or ECSA)</p>

# SEALING TECH

Taking Cyber Security Seriously

<p>58. PT-Computer Security Systems Specialist III</p>	<p>Analyzes and defines security requirements for complex engineering issues. Designs, develops, engineers, and implements solutions to system architectural requirements. Gathers and organizes technical information about an organization's mission goals and needs, existing security products, and ongoing programs. Performs risk analyses and assessments. Provides daily supervision and direction to staff. Provides technical support for secure software development and integration tasks, including reviewing work products for correctness and adhering to the design concept and to user standards. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Coordinates with system and network owners to cooperatively review architectures and provide advisement on vulnerabilities with associated remediation recommendations. Knowledgeable of Security/Information Assurance (IA) products such as PKI, VPN, firewalls, and intrusion detection systems. Analyzes and recommends resolution of security/IA problems on the basis of knowledge of the major IA products and services, an understanding of their limitations, and knowledge of the IA disciplines. Provides daily supervision and direction to staff when leading a team.</p>	<p>6 years</p>	<p>Bachelor's degree in a related field or security certification (CCNA, LPT, or CISSP)</p>
<p>59. PT- Cyber Information Assurance Specialist I</p>	<p>Under specific guidance, performs technical support focused on the development, operation, management, and enforcement of cybersecurity capabilities for systems and networks. Cybersecurity support is concentrated on the protection and defense of information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for their restoration by incorporating protection, detection, and reaction capabilities. Supports or conducts authorized penetration testing on systems and networks. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Coordinates with system and network owners to cooperatively review architectures and provide advisement on vulnerabilities with associated remediation recommendations.</p>	<p>2 years</p>	<p>At least 60 semester hours of education in a related field and a technical certification listed in DoD 8570.01 IAT level I or DoD 8570.01 IAM level I requirements</p>

<p>60. PT- Cyber Information Assurance Specialist II</p>	<p>Under general supervision, performs technical support focused on the development, operation, management, and enforcement of cybersecurity capabilities for systems and networks. Cybersecurity support is concentrated on the protection and defense of information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for their restoration by incorporating protection, detection, and reaction capabilities. Supports or conducts authorized penetration testing on systems and networks. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Coordinates with system and network owners to cooperatively review architectures and provide advisement on vulnerabilities with associated remediation recommendations</p>	<p>2 years</p>	<p>At least 60 semester hours of education in a related field and a technical certification listed in DoD 8570.01 IAT level II or DoD 8570.01 IAM level II requirements</p>
<p>61. PT- Cyber Information Assurance Specialist III</p>	<p>Works independently or manages a team of security engineers to apply advanced security knowledge to programs. Performs technical support focused on the development, operation, management, and enforcement of cybersecurity capabilities for systems and networks. Cybersecurity support is concentrated on the protection and defense of information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for their restoration by incorporating protection, detection, and reaction capabilities. Supports or conducts authorized penetration testing on systems and networks. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Coordinates with system and network owners to cooperatively review architectures and provide advisement on vulnerabilities with associated remediation recommendations.</p>	<p>6 years</p>	<p>Bachelor's degree in a related field and a technical certification listed in DoD 8570.01 IAT level II or DoD 8570.01 IAM level II requirements</p>
<p>62. PT- Cybersecurity Consultant I</p>	<p>Experience with several ADP architectures and platforms in an integrated environment. Stays current with advances in information technology. Assists in the analysis of current and projected service maintenance personnel and facility requirements. Designs interfaces to allow incompatible equipment to function as a unified system.</p>	<p>3 years</p>	<p>Bachelor's degree in a related field</p>

<p>63. PT - Cybersecurity Consultant II</p>	<p>Leads major portions of large or medium projects and leads small projects autonomously. Gathers facts through research, interviewing, surveys, etc. Analyzes the client's business, draws conclusions, prepares final reports and gives presentations. Uses in-depth consultative skills and business knowledge to practice business objectives and processes. Manages and implements large, complex information technology systems. Advises senior executives on effective utilization of information technology systems and reengineering to meet business objectives. Identifies user requirements and describes services available or refers inquiries to other staff within installation. Provides technical support of a limited scope to users and assists them in defining and solving computing problems within well-defined areas of responsibility. Assists in preparing documentation of supported products for other staff members and users. Assists in preparing user training materials and conduct training sessions as assigned.</p>	<p>4 years</p>	<p>Bachelor's degree in a related field</p>
<p>64. PT- Cybersecurity Consultant III</p>	<p>Manages the project work as defined by the client contract. Leads medium to large complex projects and major phases of very large projects. Manages the fact-finding, analysis, and development of hypothesis/conclusions, production of final reports, and delivery of presentations. Ensures that the project delivers to client expectations on time and to budget.</p>	<p>6 years</p>	<p>Bachelor's degree in a related field</p>
<p>65.PT Cybersecurity Consultant IV</p>	<p>Manages and implements large, complex information technology systems. Experienced in advising senior executives on effective utilization of information technology systems and reengineering to meet business objectives. Identifies user requirements and describes services available or refers inquiries to other staff within installation. Provides technical support of a limited scope to users and assists them in defining and solving computing problems within well-defined areas of responsibility. Assists in preparing documentation of supported products for other staff members and users. Assists in preparing user training materials and conducts training sessions as assigned. Performs programming tasks of limited scope to assist users.</p>	<p>6 years</p>	<p>Master's degree in a related field</p>

<p>66. PT-Cybersecurity Consultant V</p>	<p>Serves as a Management Information System (MIS) manager. Designs, develops and manages implementation of risk assessment and business contingency planning framework, methodology, and tools to ensure business continuity of operations across a large, multi-division, decentralized organization. Supports multi-language, multi-platform and multi-operating system operations and utilizes electronic commerce and Electronic Data Interchange (EDI) applications. Recognizes and recommends new or emerging technology or software to satisfy functional requirements and processes. Provides highly technical and/or specialized guidance concerning automation solutions to complex information processing problems related to the subject field. Provides customer support using enterprise solutions software to integrate business areas consistent with today's technology in order to operate in an open systems environment and client service architecture. Analyzes data processing requirements to plan EDP systems to provide system capabilities required for projected workloads. Plans layout and installation of new systems or modification of existing systems. May set up and control analog or hybrid computer systems to solve scientific and engineering problems. Knowledgeable in Oracle, Windows NT, network administration, project management and Unix and Cobol programming. Internet Development/Integration. Develops applications that take advantage of Internet protocols and platforms. Internet developers extend beyond traditional software development disciplines to demonstrate advanced graphical design abilities, familiarity with new media formats, and solid understanding of Internet communications protocols and services. Deploys new applications that utilize Internet standards to enable wide access from the diverse client types found throughout the public Internet</p>	<p>8 years</p>	<p>Master's degree in a related field</p>
--	--	----------------	---

<p>67. PT- Cybersecurity Consultant VI</p>	<p>Senior consultant to top level management. Viewed as the expert in discipline or related area of expertise, exhibiting an exceptional degree of ingenuity, creativity, and resourcefulness. Managerial/leadership experience required. Typically serves as the prime spokesperson to the customer. Performs technical planning, system integration, verification and validation, cost and risk, and supportability and effectiveness analyses for total systems. Analyses are performed at all levels of total system product to include: hardware/software, concept, design, fabrication, test, installation, operation, maintenance, and disposal. Performs duties such as site surveys, system evaluation, system analysis, architecture, and infrastructure assessment. Ensures the logical and systematic conversion of customer or product requirements into total systems solutions that acknowledge technical, schedule, and cost constraints. Applies and/or develops advanced technologies, scientific principles, theories, and concepts. Often acts independently to resolve issues associated with the development and implementation of operational programs. Plans R&amp;D programs and recommends technological application programs to accomplish long-range objectives</p>	<p>10 years</p>	<p>Master's degree in a related field</p>
--	---	-----------------	---

# SEALING TECH

Taking Cyber Security Seriously

<p>68. PT- Cyberspace Program Manager</p>	<p>Serves as the contractor’s single contract manager and shall be the contractor’s authorized interface with the Government Contracting Officer (CO), Government management personnel and customer agency representatives. Coordinates authorized penetration testing on systems and networks. Leads command and control functions in response to incidents. Supervises the collection of intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Oversees the coordination of incident data to identify specific vulnerabilities and recommends remediation actions. Manages teams and provides quality assurance with vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Responsible for formulating and enforcing work standards, assigning contractor schedules, reviewing work discrepancies, supervising contractor personnel and communicating policies, purposes, and goals of the organization to subordinates.</p>	<p>6 years</p>	<p>Bachelor’s degree in a related field, PMP certification</p>
<p>69. PT- Cybersecurity Subject Matter Expert I</p>	<p>Under broad direction, provides support, analysis, and research into complex problems and processes relating to the subject matter. Serves as technical advisor on high-level project teams providing technical direction, interpretation, and alternatives. Thinks independently and demonstrates superior written and oral communications skills. Possesses a complete understanding and wide experience in the application of technical principles, theories, and concepts in the field. Provides technical solutions to a wide range of difficult problems. Solutions are imaginative, thorough, practicable, and consistent with organizational objectives. Independently determines and develops approach to solutions. Contributes to the completion of specific programs and projects. Possesses expertise in a particular area of Information Technology (e.g., Penetration Testing, Incident Response, Cyber Hunt, Risk and Vulnerability Assessments).</p>	<p>4 years</p>	<p>Bachelor's Degree in a related field</p>

<p>70. PT- Cybersecurity Subject Matter Expert II</p>	<p>With minimal direction, provides Intermediate level support, analysis, and research into exceptionally complex problems and processes relating to the subject matter. Serves as technical expert on executive-level project teams providing technical direction, interpretation and alternatives. Thinks independently and demonstrates exceptional written and oral communications skills. Applies extensive technical expertise, 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. Exercises considerable latitude in determining technical objectives of assignment. Possesses expertise in a particular area of Information Technology (e.g., Penetration Testing, Incident Response, Cyber Hunt, Risk and Vulnerability Assessments).</p>	<p>6 years</p>	<p>Bachelor's degree in a related field</p>
<p>71. PT- Cybersecurity Subject Matter Expert III</p>	<p>Provides expert support, analysis, and research into exceptionally complex problems, and processes relating to the subject matter. Serves as technical expert on executive- level project teams providing technical direction, interpretation and alternatives. Thinks independently and demonstrates exceptional written and oral communications skills. Applies advanced technical principles, theories, and concepts. Contributes to the development of new principles and concepts. Works on unusually complex technical problems and provides solutions which are highly innovative. Works under consultative direction toward predetermined long-range goals and objectives. Assignments are often self- initiated. Determines and pursues courses of action necessary to obtain desired results. Develops advanced technological ideas and guides their development into a final product. Possesses expertise in a particular area of Information Technology (e.g., Penetration Testing, Incident Response, Cyber Hunt, Risk and Vulnerability Assessments).</p>	<p>4 years</p>	<p>Master's degree in a related field</p>

<p>72. PT- Cybersecurity Subject Matter Expert IV</p>	<p>Provides architecture and engineering SME support across multiple enterprise level initiatives. Determines and identifies high-level functional and technical requirements based on interactions with the user community and knowledge of the existing enterprise architecture. Designs enterprise architectures to include the software, hardware and communications to support the enterprise requirements as well as provide for present and future cross-functional requirements and interfaces. Identifies, assesses, and presents options for meeting the functional and technical requirements including hardware and software updates or upgrades.</p> <p>Develops high- level system design diagrams. Ensures systems are compatible and in compliance with the standards for open systems architectures, the Open Systems Interconnection (OSI) and International Standards Organization (ISO) reference models, and profiles of standards. Ensures compliance with standards and directives. Evaluates problems of work flows, organization and planning and develops appropriate corrective action. Evaluates and recommends new technologies.</p>	<p>6 years</p>	<p>Master’s degree in a related field</p>
<p>73. PT- Cybersecurity Training Specialist I</p>	<p>Under specific guidance, develops, plans, coordinates, delivers, and/or evaluates instructional cybersecurity content using various training methods, tactics, tools, and techniques. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments.</p>	<p>0 years</p>	<p>Associate’s degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCNA, CEH)</p>

<p>74. PT-Cybersecurity Training Specialist II</p>	<p>Under general supervision, develops, plans, coordinates, delivers, and/or evaluates instructional cybersecurity content using various training methods, tactics, tools, and techniques. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments.</p>	<p>3 years</p>	<p>Associate's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCNA, CEH)</p>
<p>75. PT-Cybersecurity Training Specialist III</p>	<p>Develops, plans, coordinates, delivers, and/or evaluates instructional cybersecurity content using various training methods, tactics, tools, and techniques. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Provides daily supervision and direction to staff when leading a team.</p>	<p>6 years</p>	<p>Bachelor's degree in Computer Science, Physics, Mathematics, Operations Research, Information</p>

76. PT- Cybersecurity Training Specialist IV	Provides expertise in cybersecurity training discipline or related area of expertise, exhibiting an exceptional degree of ingenuity, creativity, and resourcefulness. Develops, plans, coordinates, delivers, and/or evaluates instructional cybersecurity content using various training methods, tactics, tools, and techniques. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments.	12 years	Master’s degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCIE, LPT, or CISSP)
77. PT- Cybersecurity Training Specialist V	Serves as the onsite Training team lead. Designs, develops and manages implementation of cybersecurity training curriculum and materials. Senior consultant to top level management. Viewed as the expert in cybersecurity training discipline or related area of expertise, exhibiting an exceptional degree of ingenuity, creativity, and resourcefulness. Develops, plans, coordinates, delivers, and/or evaluates instructional cybersecurity content using various training methods, tactics, tools, and techniques. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments.	14 years	Master’s degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCIE, LPT, or CISSP)
78. PT- Cyber Threat Analyst I	Under specific guidance, conducts all–source analysis, digital forensics, and targeting to identify, monitor, assess, and counter the threat posed by foreign cyber actors against information systems, critical infrastructure and cyber–related	0 years	Associate’s degree in Computer Science,

	<p>interests. Produces strategic assessments and provide tactical analysis and advice for cyber and intelligence operations. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Applies scientific and technical knowledge to solve complex cyber and intelligence problems, produces short-term and long-term written assessments, and briefs decision makers to support organizational risk decision making.</p>		<p>Physics, Mathematics, Operations Research, Information Technology, or security certification (CCNA or CEH)</p>
<p>79. PT- Cyber Threat Analyst II</p>	<p>Under general supervision, conducts all-source analysis, digital forensics, and targeting to identify, monitor, assess, and counter the threat posed by foreign cyber actors against information systems, critical infrastructure and cyber-related interests. Produces strategic assessments and provide tactical analysis and advice for cyber and intelligence operations. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Applies scientific and technical knowledge to solve complex cyber and intelligence problems, produces short-term and long-term written assessments, and briefs decision makers to support organizational risk decision making.</p>	<p>3 years</p>	<p>Associate's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCNA, ECSA, or CISSP)</p>

<p>80. PT-Cyber Threat Analyst III</p>	<p>Conducts all–source analysis, digital forensics, and targeting to identify, monitor, assess, and counter the threat posed by foreign cyber actors against information systems, critical infrastructure and cyber–related interests. Produces strategic assessments and provide tactical analysis and advice for cyber and intelligence operations. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Applies scientific and technical knowledge to solve complex cyber and intelligence problems, produces short–term and long–term written assessments, and briefs decision makers to support organizational risk decision making.</p>	<p>6 years</p>	<p>Bachelor’s degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCIE, LPT, or CISSP)</p>
<p>81. PT-Cyber Threat Analyst IV</p>	<p>Provides expertise in cyber threat analysis discipline or related area of expertise, exhibiting an exceptional degree of ingenuity, creativity, and resourcefulness. Conducts all–source analysis, digital forensics, and targeting to identify, monitor, assess, and counter the threat posed by foreign cyber actors against information systems, critical infrastructure and cyber–related interests. Produces strategic assessments and provide tactical analysis and advice for cyber and intelligence operations. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Applies scientific and technical knowledge to solve complex cyber and</p>	<p>12 years</p>	<p>Master’s degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCIE, LPT, or CISSP)</p>

	intelligence problems, produces short-term and long-term written assessments, and briefs decision makers to support organizational risk decision making.		
82. PT- Defensive Cyberspace Operator I	Under specific guidance, supports activities to defend friendly cyberspace. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Performs internal defensive measures to include actively hunting for advanced internal threats as well as the internal responses to these threats. Responds to unauthorized activity or alerts/threat information, and leverages intelligence, and other capabilities as required. Performs technical and non-technical activities and actions to protect, monitor, analyze, detect, and respond to unauthorized activity within information systems and networks. Supports passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.	0 years	Associate's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCNA or CEH)

<p>83. PT- Defensive Cyberspace Operator II</p>	<p>Under general supervision, supports activities to defend friendly cyberspace. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments.</p> <p>Performs internal defensive measures to include actively hunting for advanced internal threats as well as the internal responses to these threats.</p> <p>Responds to unauthorized activity or alerts/threat information, and leverages intelligence, and other capabilities as required.</p> <p>Performs technical and non- technical activities and actions to protect, monitor, analyze, detect, and respond to unauthorized activity within information systems and networks. Supports passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.</p>	<p>3 years</p>	<p>Associate degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCNA, ECSCA, or CISSP)</p>
---	---	----------------	---

<p>84. PT- Defensive Cyberspace Operator III</p>	<p>Supports activities to defend friendly cyberspace. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Performs internal defensive measures to include actively hunting for advanced internal threats as well as the internal responses to these threats. Responds to unauthorized activity or alerts/threat information, and leverages intelligence, and other capabilities as required. Performs technical and non- technical activities and actions to protect, monitor, analyze, detect, and respond to unauthorized activity within information systems and networks. Supports passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.</p>	<p>6 years</p>	<p>Bachelor's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCIE, LPT, or CISSP)</p>
<p>85. PT- Defensive Cyberspace Operator IV</p>	<p>Provides expertise in defensive cyber operations discipline or related area of expertise, exhibiting an exceptional degree of ingenuity, creativity, and resourcefulness. Supports activities to defend friendly cyberspace. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to</p>	<p>10 years</p>	<p>Bachelor's degree in Computer Science, Physics, Mathematics,</p>

	<p>incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Performs internal defensive measures to include actively hunting for advanced internal threats as well as the internal responses to these threats. Responds to unauthorized activity or alerts/threat information, and leverages intelligence, and other capabilities as required. Performs technical and non- technical activities and actions to protect, monitor, analyze, detect, and respond to unauthorized activity within information systems and networks. Supports passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.</p>		<p>Operations Research, Information Technology, or security certification (CCIE, LPT, or CISSP)</p>
<p>86. PT- Offensive Cyberspace Operator I</p>	<p>Under specific guidance, supports information gathering and operations in and through cyberspace. Participates in independent and focused threat-based efforts that simulate an interdisciplinary, simulated adversary to expose and exploit vulnerabilities as a means to improve the cybersecurity posture of information systems and networks. Supports exercise related activities, where the cyber operator simulates an opposing force and is focused on improving readiness and asses the performance of their people executing operations supported by their technology. Supports network penetration testing activities, where cyber operator provides security testing in an attempt to primarily circumvent the technology security features of a system based on their understanding of the system design and implementation. Supports all other authorized and organized activities to emulate a potential adversary's attack or exploitation capabilities with the intent to improve enterprise cybersecurity and cyberspace operations.</p>	<p>0 years</p>	<p>Associate's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCNA or CEH)</p>

<p>87. PT- Offensive Cyberspace Operator II</p>	<p>Under general supervision, supports information gathering and operations in and through cyberspace. Participates in independent and focused threat-based efforts that simulate an interdisciplinary, simulated adversary to expose and exploit vulnerabilities as a means to improve the cybersecurity posture of information systems and networks. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions to create stimulus on target systems and networks. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Supports exercise related activities, where the cyber operator simulates an opposing force and is focused on improving readiness and assesses the performance of their people executing operations supported by their technology. Supports network penetration testing activities, where cyber operator provides security testing in an attempt to primarily circumvent the technology security features of a system based on their understanding of the system design and implementation. Supports all other authorized and organized activities to emulate a potential adversary's attack or exploitation capabilities with the intent to improve enterprise cybersecurity and cyberspace operations.</p>	<p>3 years</p>	<p>Associate's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCNA, ECSA, or CISSP)</p>
<p>88. PT- Offensive Cyberspace Operator III</p>	<p>Supports information gathering and operations in and through cyberspace. Participates in independent and focused threat-based efforts that simulate an interdisciplinary, simulated adversary to expose and exploit vulnerabilities as a means to improve the cybersecurity posture of information systems and networks. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions to create stimulus on target systems and networks. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Supports exercise related activities, where the cyber operator simulates an opposing force and is focused on improving readiness and assesses the performance of their people executing operations supported by their technology. Supports network</p>	<p>6 years</p>	<p>Bachelor's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCIE, LPT, or CISSP)</p>

	<p>penetration testing activities, where cyber operator provides security testing in an attempt to primarily circumvent the technology security features of a system based on their understanding of the system design and implementation. Supports all other authorized and organized activities to emulate a potential adversary's attack or exploitation capabilities with the intent to improve enterprise cybersecurity and cyberspace operations.</p>		
<p>89. PT- Offensive Cyberspace Operator IV</p>	<p>Provides expertise in offensive cyber operations discipline or related area of expertise, exhibiting an exceptional degree of ingenuity, creativity, and resourcefulness. Supports information gathering and operations in and through cyberspace. Participates in independent and focused threat-based efforts that simulate an interdisciplinary, simulated adversary to expose and exploit vulnerabilities as a means to improve the cybersecurity posture of information systems and networks. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions to create stimulus on target systems and networks. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Supports exercise related activities, where the cyber operator simulates an opposing force and is focused on improving readiness and assesses the performance of their people executing operations supported by their technology.</p> <p>Supports network penetration testing activities, where cyber operator provides security testing in an attempt to primarily circumvent the technology security features of a system based on their understanding of the system design and implementation. Supports all other authorized and organized activities to emulate a potential adversary's attack or exploitation capabilities with the intent to improve enterprise cybersecurity and cyberspace operations.</p>	<p>10 years</p>	<p>Bachelor's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCIE, LPT, or CISSP)</p>

# SEALING TECH

Taking Cyber Security Seriously

<p>90. IR- Computer Security Systems Specialist I</p>	<p>Under specific direction, analyzes user needs and current security regulations and guidelines to determine IA functional requirements. Provides Information Security Controls and guidelines to nodes and network management systems. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Coordinates with system and network owners to cooperatively review architectures and provide advisement on vulnerabilities with associated remediation recommendations. Maintains network/system access and password controls. Collates and analyzes audit trail data. Reviews security threats and determines/implements effective countermeasures IAW established policies/regulations/directives. Analyzes network or system changes/reconfigurations for security impacts (performs risk analysis/assessment). Documents security measures policies</p>	<p>1 year</p>	<p>Associates degree in a related field or security certification (CCNA or CEH)</p>
<p>91. IR- Computer Security Systems Specialist II</p>	<p>Under general supervision, analyzes and defines security requirements. Provides Information Security Controls and guidelines to nodes and network management systems. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Coordinates with system and network owners to cooperatively review architectures and provide advisement on vulnerabilities with associated remediation recommendations. Maintains network/system access and password controls. Collates and analyzes audit trail data. Reviews security threats and determines/implements effective countermeasures IAW established policies/regulations/directives. Analyzes network or system changes/reconfigurations for security impacts (performs risk analysis/assessment). Documents security measures policies. Knowledgeable of Security/IA products such as PKI, VPN, firewalls, and intrusion detection systems. Analyzes and recommends resolution of security/IA problems on the basis of knowledge of the major IA products and services, an understanding of their limitations, and knowledge of the IA disciplines.</p>	<p>3 years</p>	<p>Bachelor's degree in a related field or security certification (CCNA or ECSA)</p>

# SEALING TECH

Taking Cyber Security Seriously

<p>92. IR- Computer Security Systems Specialist III</p>	<p>Analyzes and defines security requirements for complex engineering issues. Designs, develops, engineers, and implements solutions to system architectural requirements. Gathers and organizes technical information about an organization's mission goals and needs, existing security products, and ongoing programs. Performs risk analyses and assessments. Provides daily supervision and direction to staff. Provides technical support for secure software development and integration tasks, including reviewing work products for correctness and adhering to the design concept and to user standards. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Coordinates with system and network owners to cooperatively review architectures and provide advisement on vulnerabilities with associated remediation recommendations. Knowledgeable of Security/Information Assurance (IA) products such as PKI, VPN, firewalls, and intrusion detection systems. Analyzes and recommends resolution of security/IA problems on the basis of knowledge of the major IA products and services, an understanding of their limitations, and knowledge of the IA disciplines. Provides daily supervision and direction to staff when leading a team.</p>	<p>6 years</p>	<p>Bachelor's degree in a related field or security certification (CCIE, LPT, or CISSP)</p>
<p>93. IR- Cybersecurity Consultant I</p>	<p>Experience with several ADP architectures and platforms in an integrated environment. Stays current with advances in information technology. Assists in the analysis of current and projected service maintenance personnel and facility requirements. Designs interfaces to allow incompatible equipment to function as a unified system.</p>	<p>3 years</p>	<p>Bachelor's degree in a related field</p>

<p>94. IR-Cybersecurity Consultant II</p>	<p>Leads major portions of large or medium projects and leads small projects autonomously. Gathers facts through research, interviewing, surveys, etc. Analyzes the client's business, draws conclusions, prepares final reports and gives presentations. Uses in-depth consultative skills and business knowledge to practice business objectives and processes. Manages and implements large, complex information technology systems. Advises senior executives on effective utilization of information technology systems and reengineering to meet business objectives. Identifies user requirements and describes services available or refers inquiries to other staff within installation. Provides technical support of a limited scope to users and assists them in defining and solving computing problems within well-defined areas of responsibility. Assists in preparing documentation of supported products for other staff members and users. Assists in preparing user training materials and conduct training sessions as assigned. Performs programming tasks of limited scope to assist users</p>	<p>4 years</p>	<p>Bachelor's degree in a related field</p>
<p>95. IR-Cybersecurity Consultant III</p>	<p>Manages the project work as defined by the client contract. Leads medium to large complex projects and major phases of very large projects. Manages the fact-finding, analysis, and development of hypothesis/conclusions, production of final reports, and delivery of presentations. Ensures that the project delivers to client expectations on time and to budget.</p>	<p>6 years</p>	<p>Bachelor's degree in a related field</p>
<p>96. IR-Cybersecurity Consultant IV</p>	<p>Manages and implements large, complex information technology systems. Experienced in advising senior executives on effective utilization of information technology systems and reengineering to meet business objectives. Identifies user requirements and describes services available or refers inquiries to other staff within installation. Provides technical support of a limited scope to users and assists them in defining and solving computing problems within well-defined areas of responsibility. Assists in preparing documentation of supported products for other staff members and users. Assists in preparing user training materials and conducts training sessions as assigned. Performs programming tasks of limited scope to assist users.</p>	<p>6 years</p>	<p>Master's degree in a related field</p>

<p>97. IR-Cybersecurity Consultant V</p>	<p>Serves as a Management Information System (MIS) manager. Designs, develops and manages implementation of risk assessment and business contingency planning framework, methodology, and tools to ensure business continuity of operations across a large, multi-division, decentralized organization. Supports multi-language, multi-platform and multi-operating system operations and utilizes electronic commerce and Electronic Data Interchange (EDI) applications. Recognizes and recommends new or emerging technology or software to satisfy functional requirements and processes. Provides highly technical and/or specialized guidance concerning automation solutions to complex information processing problems related to the subject field. Provides customer support using enterprise solutions software to integrate business areas consistent with today's technology in order to operate in an open systems environment and client service architecture. Analyzes data processing requirements to plan EDP systems to provide system capabilities required for projected workloads. Plans layout and installation of new systems or modification of existing systems. May set up and control analog or hybrid computer systems to solve scientific and engineering problems. Knowledgeable in Oracle, Windows NT, network administration, project management and Unix and Cobol programming. Internet Development/Integration. Develops applications that take advantage of Internet protocols and platforms. Internet developers extend beyond traditional software development disciplines to demonstrate advanced graphical design abilities, familiarity with new media formats, and solid understanding of Internet communications protocols and services. Deploys new applications that utilize Internet standards to enable wide access from the diverse client types found throughout the public Internet</p>	<p>8 years</p>	<p>Master's degree in a related field</p>
--	--	----------------	---

<p>98. IR-Cybersecurity Consultant VI</p>	<p>Senior consultant to top level management. Viewed as the expert in discipline or related area of expertise, exhibiting an exceptional degree of ingenuity, creativity, and resourcefulness. Managerial/leadership experience required. Typically serves as the prime spokesperson to the customer. Performs technical planning, system integration, verification and validation, cost and risk, and supportability and effectiveness analyses for total systems. Analyses are performed at all levels of total system product to include: hardware/software, concept, design, fabrication, test, installation, operation, maintenance, and disposal. Performs duties such as site surveys, system evaluation, system analysis, architecture, and infrastructure assessment. Ensures the logical and systematic conversion of customer or product requirements into total systems solutions that acknowledge technical, schedule, and cost constraints. Applies and/or develops advanced technologies, scientific principles, theories, and concepts. Often acts independently to resolve issues associated with the development and implementation of operational programs. Plans R&amp;D programs and recommends technological application programs to accomplish long-range objectives.</p>	<p>10 years</p>	<p>Master's degree in a related field</p>
<p>99. IR-Cyberspace Program Manager</p>	<p>Serves as the contractor's single contract manager and shall be the contractor's authorized interface with the Government Contracting Officer (CO), Government management personnel and customer agency representatives. Coordinates authorized penetration testing on systems and networks. Leads command and control functions in response to incidents</p>	<p>6 years</p>	<p>Bachelor's degree in a related field, PMP certification</p>

	<p>Supervises the collection of intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Oversees the coordination of incident data to identify specific vulnerabilities and recommends remediation actions. Manages teams and provides quality assurance with vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Responsible for formulating and enforcing work standards, assigning contractor schedules, reviewing work discrepancies, supervising contractor personnel and communicating policies, purposes, and goals of the organization to subordinates.</p>		
<p>100. IR-Cybersecurity Subject Matter Expert I</p>	<p>Under broad direction, provides support, analysis, and research into complex problems and processes relating to the subject matter. Serves as technical advisor on high-level project teams providing technical direction, interpretation, and alternatives. Thinks independently and demonstrates superior written and oral communications skills. Possesses a complete understanding and wide experience in the application of technical principles, theories, and concepts in the field. Provides technical solutions to a wide range of difficult problems. Solutions are imaginative, thorough, practicable, and consistent with organizational objectives. Independently determines and develops approach to solutions. Contributes to the completion of specific programs and projects. Possesses expertise in a particular area of Information Technology (e.g., Penetration Testing, Incident Response, Cyber Hunt, Risk and Vulnerability Assessments).</p>	<p>4 years</p>	<p>Bachelor's Degree in a related field</p>

<p>101. IR- Cybersecurity Subject Matter Expert II</p>	<p>With minimal direction, provides Intermediate level support, analysis, and research into exceptionally complex problems and processes relating to the subject matter. Serves as technical expert on executive-level project teams providing technical direction, interpretation and alternatives. Thinks independently and demonstrates exceptional written and oral communications skills. Applies extensive technical expertise 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. Exercises considerable latitude in determining technical objectives of assignment. Possesses expertise in a particular area of Information Technology (e.g., Penetration Testing, Incident Response, Cyber Hunt, Risk and Vulnerability Assessments).</p>	<p>6 years</p>	<p>Bachelor's degree in a related field</p>
<p>102. IR- Cybersecurity Subject Matter Expert III</p>	<p>Provides expert support, analysis, and research into exceptionally complex problems, and processes relating to the subject matter. Serves as technical expert on executive- level project teams providing technical direction, interpretation and alternatives. Thinks independently and demonstrates exceptional written and oral communications skills. Applies advanced technical principles, theories, and concepts. Contributes to the development of new principles and concepts. Works on unusually complex technical problems and provides solutions which are highly innovative. Works under consultative direction toward predetermined long-range goals and objectives. Assignments are often self- initiated. Determines and pursues courses of action necessary to obtain desired results. Develops advanced technological ideas and guides their development into a final product. Possesses expertise in a particular area of Information Technology (e.g., Penetration Testing, Incident Response, Cyber Hunt, Risk and Vulnerability Assessments).</p>	<p>4 years</p>	<p>Master's degree in a related field</p>

<p>103. IR-Cybersecurity Subject Matter Expert IV</p>	<p>Provides architecture and engineering SME support across multiple enterprise level initiatives. Determines and identifies high-level functional and technical requirements based on interactions with the user community and knowledge of the existing enterprise architecture. Designs enterprise architectures to include the software, hardware and communications to support the enterprise requirements as well as provide for present and future cross-functional requirements and interfaces. Identifies, assesses, and presents options for meeting the functional and technical requirements including hardware and software updates or upgrades. Develops high-level system design diagrams. Ensures systems are compatible and in compliance with the standards for open systems architectures, the Open Systems Interconnection (OSI) and International Standards Organization (ISO) reference models, and profiles of standards. Ensures compliance with standards and directives. Evaluates problems of work flows, organization and planning and develops appropriate corrective action. Evaluates and recommends new technologies</p>	<p>6 years</p>	<p>Master's degree in a related field</p>
---	--	----------------	---

<p>104. IR- Cyber Threat Analyst I</p>	<p>Under specific guidance, conducts all–source analysis, digital forensics, and targeting to identify, monitor, assess, and counter the threat posed by foreign cyber actors against information systems, critical infrastructure and cyber–related interests. Produces strategic assessments and provide tactical analysis and advice for cyber and intelligence operations. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Applies scientific and technical knowledge to solve complex cyber and intelligence problems, produces short–term and long–term written assessments, and briefs decision makers to support organizational risk decision making.</p>	<p>0 years</p>	<p>Associate’s degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCNA or CEH)</p>
<p>105. IR- Cyber Threat Analyst II</p>	<p>Under general supervision, conducts all–source analysis, digital forensics, and targeting to identify, monitor, assess, and counter the threat posed by foreign cyber actors against information systems, critical infrastructure and cyber–related interests. Produces strategic assessments and provide tactical analysis and advice for cyber and intelligence operations. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments,</p>	<p>3 years</p>	<p>Associate’s degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCNA or ECSA)</p>

	web application assessments, and network perimeter protection assessments. Applies scientific and technical knowledge to solve complex cyber and intelligence problems, produces short-term and long-term written assessments, and briefs decision makers to support organizational risk decision making.		
106. IR- Cyber Threat Analyst III	Conducts all-source analysis, digital forensics, and targeting to identify, monitor, assess, and counter the threat posed by foreign cyber actors against information systems, critical infrastructure and cyber-related interests. Produces strategic assessments and provide tactical analysis and advice for cyber and intelligence operations. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Applies scientific and technical knowledge to solve complex cyber and intelligence problems, produces short-term and long-term written assessments, and briefs decision makers to support organizational risk decision making.	6 years	Bachelor's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCIE, LPT, or CISSP)

<p>107. IR- Cyber Threat Analyst IV</p>	<p>Provides expertise in cyber threat analysis discipline or related area of expertise, exhibiting an exceptional degree of ingenuity, creativity, and resourcefulness. Conducts all-source analysis, digital forensics, and targeting to identify, monitor, assess, and counter the threat posed by foreign cyber actors against information systems, critical infrastructure and cyber-related interests. Produces strategic assessments and provide tactical analysis and advice for cyber and intelligence operations. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Applies scientific and technical knowledge to solve complex cyber and intelligence problems, produces short-term and long-term written assessments, and briefs decision makers to support organizational risk decision making</p>	<p>12 years</p>	<p>Master's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCIE, LPT, or CISSP)</p>
---	---	-----------------	--

<p>108. IR-Defensive Cyberspace Operator I</p>	<p>Under specific guidance, supports activities to defend friendly cyberspace. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Performs internal defensive measures to include actively hunting for advanced internal threats as well as the internal responses to these threats. Responds to unauthorized activity or alerts/threat information, and leverages intelligence, and other capabilities as required. Performs technical and non-technical activities and actions to protect, monitor, analyze, detect, and respond to unauthorized activity within information systems and networks. Supports passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.</p>	<p>0 years</p>	<p>Associate's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCNA or CEH)</p>
<p>109. IR-Defensive Cyberspace Operator II</p>	<p>Under general supervision, supports activities to defend friendly cyberspace. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates</p>	<p>3 years</p>	<p>Associate's degree in Computer Science, Physics, Mathematics, Operations Research,</p>

	<p>incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Performs internal defensive measures to include actively hunting for advanced internal threats as well as the internal responses to these threats. Responds to unauthorized activity or alerts/threat information, and leverages intelligence, and other capabilities as required.</p> <p>Performs technical and non- technical activities and actions to protect, monitor, analyze, detect, and respond to unauthorized activity within information systems and networks. Supports passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.</p>		<p>Information Technology, or security certification (CCNA or CEH)</p>
<p>110. IR-Defensive Cyberspace Operator III</p>	<p>Supports activities to defend friendly cyberspace. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Performs internal defensive measures to include actively hunting for advanced internal threats as well as the internal responses to these threats. Responds to unauthorized activity or alerts/threat information, and leverages intelligence, and other capabilities as required. Performs technical and non- technical activities and actions to protect, monitor, analyze, detect, and respond to unauthorized activity within information systems and networks. Supports passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.</p>	<p>6 years</p>	<p>Bachelor's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCNA or ECSA)</p>

<p>111. IR-Defensive Cyberspace Operator IV</p>	<p>Provides expertise in defensive cyber operations discipline or related area of expertise, exhibiting an exceptional degree of ingenuity, creativity, and resourcefulness. Supports activities to defend friendly cyberspace. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Performs internal defensive measures to include actively hunting for advanced internal threats as well as the internal responses to these threats. Responds to unauthorized activity or alerts/threat information, and leverages intelligence, and other capabilities as required. Performs technical and non- technical activities and actions to protect, monitor, analyze, detect, and respond to unauthorized activity within information systems and networks. Supports passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.</p>	<p>10 years</p>	<p>Bachelor's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCIE, LPT, or CISSP)</p>
<p>112. CH-Computer Security Systems Specialist I</p>	<p>Under specific direction, analyzes user needs and current security regulations and guidelines to determine IA functional requirements. Provides Information Security Controls and guidelines to nodes and network management systems. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Coordinates with system and network owners to cooperatively review architectures and provide advisement on vulnerabilities with associated remediation recommendations. Maintains network/system access and password controls. Collates and analyzes audit trail data.</p>	<p>1 year</p>	<p>Associates degree in a related field or industry security certification (CCNA or CEH)</p>

	<p>Reviews security threats and determines/implements effective countermeasures IAW established policies/regulations/directives. Analyzes network or system changes/reconfigurations for security impacts (performs risk analysis/assessment). Documents security measures policies.</p>		
<p>113. CH-Computer Security Systems Specialist II</p>	<p>Under general supervision, analyzes and defines security requirements. Provides Information Security Controls and guidelines to nodes and network management systems. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Coordinates with system and network owners to cooperatively review architectures and provide advisement on vulnerabilities with associated remediation recommendations. Maintains network/system access and password controls. Collates and analyzes audit trail data. Reviews security threats and determines/implements effective countermeasures IAW established policies/regulations/directives. Analyzes network or system changes/reconfigurations for security impacts (performs risk analysis/assessment). Documents security measures policies. Knowledgeable of Security/IA products such as PKI, VPN, firewalls, and intrusion detection systems. Analyzes and recommends resolution of security/IA problems on the basis of knowledge of the major IA products and services, an understanding of their limitations, and knowledge of the IA disciplines.</p>	<p>3 years</p>	<p>Bachelor's degree in a related field or industry security certification (CCNA or ECSA)</p>

<p>114. CH-Computer Security Systems Specialist III</p>	<p>Analyzes and defines security requirements for complex engineering issues. Designs, develops, engineers, and implements solutions to system architectural requirements. Gathers and organizes technical information about an organization's mission goals and needs, existing security products, and ongoing programs. Performs risk analyses and assessments. Provides daily supervision and direction to staff. Provides technical support for secure software development and integration tasks, including reviewing work products for correctness and adhering to the design concept and to user standards. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Coordinates with system and network owners to cooperatively review architectures and provide advisement on vulnerabilities with associated remediation recommendations. Knowledgeable of Security/Information Assurance (IA) products such as PKI, VPN, firewalls, and intrusion detection systems. Analyzes and recommends resolution of security/IA problems on the basis of knowledge of the major IA products and services, an understanding of their limitations, and knowledge of the IA disciplines. Provides daily supervision and direction to staff when leading a team.</p>	<p>6 years</p>	<p>Bachelor's degree in a related field or industry standard security certification (CCIE, LPT, or CISSP)</p>
<p>115. CH Cybersecurity Consultant I</p>	<p>Experience with several ADP architectures and platforms in an integrated environment. Stays current with advances in information technology. Assists in the analysis of current and projected service maintenance personnel and facility requirements. Designs interfaces to allow incompatible equipment to function as a unified system.</p>	<p>3 years</p>	<p>Bachelor's degree in a related field</p>

<p>116. CH-Cybersecurity Consultant II</p>	<p>Leads major portions of large or medium projects and leads small projects autonomously. Gathers facts through research, interviewing, surveys, etc. Analyzes the client’s business, draws conclusions, prepares final reports and gives presentations. Uses in-depth consultative skills and business knowledge to practice business objectives and processes. Manages and implements large, complex information technology systems. Advises senior executives on effective utilization of information technology systems and reengineering to meet business objectives. Identifies user requirements and describes services available or refers inquiries to other staff within installation. Provides technical support of a limited scope to users and assists them in defining and solving computing problems within well-defined areas of responsibility. Assists in preparing documentation of supported products for other staff members and users. Assists in preparing user training materials and conduct training sessions as assigned. Performs programming tasks of limited scope to assist users.</p>	<p>4 years</p>	<p>Bachelor’s degree in a related field</p>
<p>117. CH-Cybersecurity Consultant III</p>	<p>Manages the project work as defined by the client contract. Leads medium to large complex projects and major phases of very large projects. Manages the fact-finding, analysis, and development of hypothesis/conclusions, production of final reports, and delivery of presentations. Ensures that the project delivers to client expectations on time and to budget.</p>	<p>6 years</p>	<p>Bachelor’s degree in a related field</p>
<p>118. CH-Cybersecurity Consultant IV</p>	<p>Manages and implements large, complex information technology systems. Experienced in advising senior executives on effective utilization of information technology systems and reengineering to meet business objectives. Identifies user requirements and describes services available or refers inquiries to other staff within installation. Provides technical support of a limited scope to users and assists them in defining and solving computing problems within well-defined areas of responsibility. Assists in preparing documentation of supported products for other staff members and users. Assists in preparing user training materials and conducts training sessions as assigned. Performs programming tasks of limited scope to assist users.</p>	<p>6 years</p>	<p>Master’s degree in a related field</p>

<p>119. CH-Cybersecurity Consultant V</p>	<p>Serves as a Management Information System (MIS) manager. Designs, develops and manages implementation of risk assessment and business contingency planning framework, methodology, and tools to ensure business continuity of operations across a large, multi-division, decentralized organization. Supports multi-language, multi-platform and multi-operating system operations and utilizes electronic commerce and Electronic Data Interchange (EDI) applications. Recognizes and recommends new or emerging technology or software to satisfy functional requirements and processes. Provides highly technical and/or specialized guidance concerning automation solutions to complex information processing problems related to the subject field. Provides customer support using enterprise solutions software to integrate business areas consistent with today's technology in order to operate in an open systems environment and client service architecture. Analyzes data processing requirements to plan EDP systems to provide system capabilities required for projected workloads. Plans layout and installation of new systems or modification of existing systems. May set up and control analog or hybrid computer systems to solve scientific and engineering problems. Knowledgeable in Oracle, Windows NT, network administration, project management and Unix and Cobol programming. Internet Development/Integration. Develops applications that take advantage of Internet protocols and platforms. Internet developers extend beyond traditional software development disciplines to demonstrate advanced graphical design abilities, familiarity with new media formats, and solid understanding of Internet communications protocols and services. Deploys new applications that utilize Internet standards to enable wide access from the diverse client types found throughout the public Internet</p>	<p>8 years</p>	<p>Master's degree in a related field</p>
---	--	----------------	---

<p>120. CH-Cybersecurity Consultant VI</p>	<p>Senior consultant to top level management. Viewed as the expert in discipline or related area of expertise, exhibiting an exceptional degree of ingenuity, creativity, and resourcefulness. Managerial/leadership experience required. Typically serves as the prime spokesperson to the customer. Performs technical planning, system integration, verification and validation, cost and risk, and supportability and effectiveness analyses for total systems. Analyses are performed at all levels of total system product to include: hardware/software, concept, design, fabrication, test, installation, operation, maintenance, and disposal. Performs duties such as site surveys, system evaluation, system analysis, architecture, and infrastructure assessment. Ensures the logical and systematic conversion of customer or product requirements into total systems solutions that acknowledge technical, schedule, and cost constraints. Applies and/or develops advanced technologies, scientific principles, theories, and concepts. Often acts independently to resolve issues associated with the development and implementation of operational programs. Plans R&amp;D programs and recommends technological application programs to accomplish long-range objectives.</p>	<p>10 years</p>	<p>Master's degree in a related field</p>
<p>121. CH-Cyberspace Program Manager</p>	<p>Serves as the contractor's single contract manager and shall be the contractor's authorized interface with the Government Contracting Officer (CO), Government management personnel and customer agency representatives. Coordinates authorized penetration testing on systems and networks. Leads command and control functions in response to incidents. Supervises the collection of intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat</p>	<p>6 years</p>	<p>Bachelor's degree in a related field, PMP certification</p>

	<p>identification attribution of CND incidents. Oversees the coordination of incident data to identify specific vulnerabilities and recommends remediation actions. Manages teams and provides quality assurance with vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Responsible for formulating and enforcing work standards, assigning contractor schedules, reviewing work discrepancies, supervising contractor personnel and communicating policies, purposes, and goals of the organization to subordinates.</p>		
<p>122. CH-Cybersecurity Subject Matter Expert I</p>	<p>Under broad direction, provides support, analysis, and research into complex problems and processes relating to the subject matter. Serves as technical advisor on high-level project teams providing technical direction, interpretation, and alternatives. Thinks independently and demonstrates superior written and oral communications skills. Possesses a complete understanding and wide experience in the application of technical principles, theories, and concepts in the field. Provides technical solutions to a wide range of difficult problems. Solutions are imaginative, thorough, practicable, and consistent with organizational objectives. Independently determines and develops approach to solutions. Contributes to the completion of specific programs and projects. Possesses expertise in a particular area of Information Technology (e.g., Penetration Testing, Incident Response, Cyber Hunt, Risk and Vulnerability Assessments).</p>	<p>4 years</p>	<p>Bachelor's Degree in a related field</p>

<p>123. CH-Cybersecurity Subject Matter Expert II</p>	<p>With minimal direction, provides Intermediate level support, analysis, and research into exceptionally complex problems and processes relating to the subject matter. Serves as technical expert on executive-level project teams providing technical direction, interpretation and alternatives. Thinks independently and demonstrates exceptional written and oral communications skills. Applies extensive technical expertise, 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. Exercises considerable latitude in determining technical objectives of assignment. Possesses expertise in a particular area of Information Technology (e.g., Penetration Testing, Incident Response, Cyber Hunt, Risk and Vulnerability Assessments)</p>	<p>6 years</p>	<p>Bachelor's degree in a related field</p>
<p>124. CH-Cybersecurity Subject Matter Expert III</p>	<p>Provides expert support, analysis, and research into exceptionally complex problems, and processes relating to the subject matter. Serves as technical expert on executive-level project teams providing technical direction, interpretation and alternatives. Thinks independently and demonstrates exceptional written and oral communications skills. Applies advanced technical principles, theories, and concepts. Contributes to the development of new principles and concepts. Works on unusually complex technical problems and provides solutions which are highly innovative. Works under consultative direction toward predetermined long-range goals and objectives. Assignments are often self-initiated. Determines and pursues courses of action necessary to obtain desired results. Develops advanced technological ideas and guides their development into a final product. Possesses expertise in a particular area of Information Technology (e.g., Penetration Testing, Incident Response, Cyber Hunt, Risk and Vulnerability Assessments).</p>	<p>4 years</p>	<p>Master's degree in a related field</p>

<p>125. CH-Cybersecurity Subject Matter Expert IV</p>	<p>Provides architecture and engineering SME support across multiple enterprise level initiatives. Determines and identifies high-level functional and technical requirements based on interactions with the user community and knowledge of the existing enterprise architecture. Designs enterprise architectures to include the software, hardware and communications to support the enterprise requirements as well as provide for present and future cross-functional requirements and interfaces. Identifies, assesses, and presents options for meeting the functional and technical requirements including hardware and software updates or upgrades. Develops high-level system design diagrams. Ensures systems are compatible and in compliance with the standards for open systems architectures, the Open Systems Interconnection (OSI) and International Standards Organization (ISO) reference models, and profiles of standards. Ensures compliance with standards and directives. Evaluates problems of work flows, organization and planning and develops appropriate corrective action. Evaluates and recommends new technologies.</p>	<p>6 years</p>	<p>Master's degree in a related field</p>
---	---	----------------	---

<p>126. CH- Cyber Threat Analyst I</p>	<p>Under specific guidance, conducts all–source analysis, digital forensics, and targeting to identify, monitor, assess, and counter the threat posed by foreign cyber actors against information systems, critical infrastructure and cyber–related interests. Produces strategic assessments and provide tactical analysis and advice for cyber and intelligence operations. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Applies scientific and technical knowledge to solve complex cyber and intelligence problems, produces short–term and long–term written assessments, and briefs decision makers to support organizational risk decision making.</p>	<p>0 years</p>	<p>Associate’s degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCNA or CEH)</p>
<p>127. CH- Cyber Threat Analyst II</p>	<p>Under general supervision, conducts all–source analysis, digital forensics, and targeting to identify, monitor, assess, and counter the threat posed by foreign cyber actors against information systems, critical infrastructure and cyber–related interests. Produces strategic assessments and provide tactical analysis and advice for cyber and intelligence operations. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Applies scientific and technical knowledge to solve complex cyber and intelligence problems, produces short–term and long–term written assessments, and briefs decision makers to support organizational risk decision making</p>	<p>3</p>	<p>Associate’s degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCNA or ECSA)</p>

<p>128. CH- Cyber Threat Analyst III</p>	<p>Conducts all-source analysis, digital forensics, and targeting to identify, monitor, assess, and counter the threat posed by foreign cyber actors against information systems, critical infrastructure and cyber-related interests. Produces strategic assessments and provide tactical analysis and advice for cyber and intelligence operations. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Applies scientific and technical knowledge to solve complex cyber and intelligence problems, produces short-term and long-term written assessments, and briefs decision makers to support organizational risk decision making.</p>	<p>6 years</p>	<p>Bachelor's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCIE, LPT, or CISSP)</p>
--	---	----------------	--

<p>129. CH- Cyber Threat Analyst IV</p>	<p>Provides expertise in cyber threat analysis discipline or related area of expertise, exhibiting an exceptional degree of ingenuity, creativity, and resourcefulness. Conducts all-source analysis, digital forensics, and targeting to identify, monitor, assess, and counter the threat posed by foreign cyber actors against information systems, critical infrastructure and cyber-related interests. Produces strategic assessments and provide tactical analysis and advice for cyber and intelligence operations. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Applies scientific and technical knowledge to solve complex cyber and intelligence problems, produces short-term and long-term written assessments, and briefs decision makers to support organizational risk decision making.</p>	<p>12 years</p>	<p>Master's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCIE, LPT, or CISSP)</p>
---	--	-----------------	--

<p>130. CH-Defensive Cyberspace Operator I</p>	<p>Under specific guidance, supports activities to defend friendly cyberspace. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Performs internal defensive measures to include actively hunting for advanced internal threats as well as the internal responses to these threats. Responds to unauthorized activity or alerts/threat information, and leverages intelligence, and other capabilities as required. Performs technical and non-technical activities and actions to protect, monitor, analyze, detect, and respond to unauthorized activity within information systems and networks. Supports passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.</p>	<p>0 years</p>	<p>Associate's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCNA or CEH)</p>
<p>131. CH-Defensive Cyberspace Operator II</p>	<p>Under general supervision, supports activities to defend friendly cyberspace. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability</p>	<p>3 years</p>	<p>Associate's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology,</p>

	<p>scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Performs internal defensive measures to include actively hunting for advanced internal threats as well as the internal responses to these threats. Responds to unauthorized activity or alerts/threat information, and leverages intelligence, and other capabilities as required.</p> <p>Performs technical and non- technical activities and actions to protect, monitor, analyze, detect, and respond to unauthorized activity within information systems and networks. Supports passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.</p>		<p>or security certification (CCNA or ECSA)</p>
<p>132. CH-Defensive Cyberspace Operator III</p>	<p>Supports activities to defend friendly cyberspace. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions.</p> <p>Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Performs internal defensive measures to include actively hunting for advanced internal threats as well as the internal responses to these threats. Responds to unauthorized activity or alerts/threat information, and leverages intelligence, and other capabilities as required. Performs technical and non- technical activities and actions to protect, monitor, analyze, detect, and respond to unauthorized activity within information systems and networks. Supports passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.</p>	<p>6 years</p>	<p>Bachelor's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCIE, LPT, or CISSP)</p>

<p>133. CH-Defensive Cyberspace Operator IV</p>	<p>Provides expertise in defensive cyber operations discipline or related area of expertise, exhibiting an exceptional degree of ingenuity, creativity, and resourcefulness. Supports activities to defend friendly cyberspace. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Performs internal defensive measures to include actively hunting for advanced internal threats as well as the internal responses to these threats. Responds to unauthorized activity or alerts/threat information, and leverages intelligence, and other capabilities as required. Performs technical and non- technical activities and actions to protect, monitor, analyze, detect, and respond to unauthorized activity within information systems and networks. Supports passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.</p>	<p>10 years</p>	<p>Bachelor's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCIE, LPT, or CISSP)</p>
<p>134. CH-Offensive Cyberspace Operator I</p>	<p>Under specific guidance, supports information gathering and operations in and through cyberspace. Participates in independent and focused threat-based efforts that simulate an interdisciplinary, simulated adversary to expose and exploit vulnerabilities as a means to improve the cybersecurity posture of information systems and networks. Supports exercise related activities, where the cyber operator simulates an opposing force and is focused on improving readiness and asses the performance of their people executing operations supported by their technology. Supports network penetration testing activities, where cyber operator provides security testing in an attempt to primarily circumvent the technology security features of a system based on their understanding of the system design and implementation. Supports all other authorized and organized activities to emulate a potential adversary's attack or exploitation capabilities with the intent to improve enterprise cybersecurity and cyberspace operations</p>	<p>0 years</p>	<p>Associate's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCNA or CEH)</p>

<p>135. CH-Offensive Cyberspace Operator II</p>	<p>Under general supervision, supports information gathering and operations in and through cyberspace. Participates in independent and focused threat-based efforts that simulate an interdisciplinary, simulated adversary to expose and exploit vulnerabilities as a means to improve the cybersecurity posture of information systems and networks. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions to create stimulus on target systems and networks. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Supports exercise related activities, where the cyber operator simulates an opposing force and is focused on improving readiness and assesses the performance of their people executing operations supported by their technology. Supports network penetration testing activities, where cyber operator provides security testing in an attempt to primarily circumvent the technology security features of a system based on their understanding of the system design and implementation. Supports all other authorized and organized activities to emulate a potential adversary's attack or exploitation capabilities with the intent to improve enterprise cybersecurity and cyberspace operations.</p>	<p>3 years</p>	<p>Associate's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCNA or ECSCA)</p>
---	---	----------------	---

<p>136. CH-Offensive Cyberspace Operator III</p>	<p>Supports information gathering and operations in and through cyberspace. Participates in independent and focused threat-based efforts that simulate an interdisciplinary, simulated adversary to expose and exploit vulnerabilities as a means to improve the cybersecurity posture of information systems and networks. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions to create stimulus on target systems and networks. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Supports exercise related activities, where the cyber operator simulates an opposing force and is focused on improving readiness and asses the performance of their people executing operations supported by their technology. Supports network penetration testing activities, where cyber operator provides security testing in an attempt to primarily circumvent the technology security features of a system based on their understanding of the system design and implementation. Supports all other authorized and organized activities to emulate a potential adversary's attack or exploitation capabilities with the intent to improve enterprise cybersecurity and cyberspace operations</p>	<p>6 years</p>	<p>Bachelor's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCIE, LPT, or CISSP)</p>
--	--	----------------	--

<p>137. CH-Offensive Cyberspace Operator IV</p>	<p>Provides expertise in offensive cyber operations discipline or related area of expertise, exhibiting an exceptional degree of ingenuity, creativity, and resourcefulness. Supports information gathering and operations in and through cyberspace. Participates in independent and focused threat-based efforts that simulate an interdisciplinary, simulated adversary to expose and exploit vulnerabilities as a means to improve the cybersecurity posture of information systems and networks. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions to create stimulus on target systems and networks. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Supports exercise related activities, where the cyber operator simulates an opposing force and is focused on improving readiness and asses the performance of their people executing operations supported by their technology.</p> <p>Supports network penetration testing activities, where cyber operator provides security testing in an attempt to primarily circumvent the technology security features of a system based on their understanding of the system design and implementation. Supports all other authorized and organized activities to emulate a potential adversary's attack or exploitation capabilities with the intent to improve enterprise cybersecurity and cyberspace operations.</p>	<p>10 years</p>	<p>Bachelor's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCIE, LPT, or CISSP)</p>
---	--	-----------------	--

<p>138. RVA-Computer Security Systems Specialist I</p>	<p>Under specific direction, analyzes user needs and current security regulations and guidelines to determine IA functional requirements. Provides Information Security Controls and guidelines to nodes and network management systems. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Coordinates with system and network owners to cooperatively review architectures and provide advisement on vulnerabilities with associated remediation recommendations. Maintains network/system access and password controls. Collates and analyzes audit trail data. Reviews security threats and determines/implements effective countermeasures IAW established policies/regulations/directives. Analyzes network or system changes/reconfigurations for security impacts (performs risk analysis/assessment). Documents security measures policies.</p>	<p>1 year</p>	<p>Associates degree in a related field or security certification (CCNA or CEH)</p>
<p>139. RVA-Computer Security Systems Specialist II</p>	<p>Under general supervision, analyzes and defines security requirements. Provides Information Security Controls and guidelines to nodes and network management systems. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Coordinates with system and network owners to cooperatively review architectures and provide advisement on vulnerabilities with associated remediation recommendations. Maintains network/system access and password controls. Collates and analyzes audit trail data. Reviews security threats and determines/implements effective countermeasures IAW established policies/regulations/directives. Analyzes network or system changes/reconfigurations for security impacts (performs risk analysis/assessment). Documents security measures policies. Knowledgeable of Security/IA products such as PKI, VPN, firewalls, and intrusion detection systems. Analyzes and recommends resolution of security/IA problems on the basis of knowledge of the major IA products and</p>	<p>3 years</p>	<p>Bachelor's degree in a related field or security certification (CCNA or ECSA)</p>

	<p>services, an understanding of their limitations, and knowledge of the IA disciplines.</p>		
<p>140. RVA-Computer Security Systems Specialist III</p>	<p>Analyzes and defines security requirements for complex engineering issues. Designs, develops, engineers, and implements solutions to system architectural requirements. Gathers and organizes technical information about an organization's mission goals and needs, existing security products, and ongoing programs. Performs risk analyses and assessments. Provides daily supervision and direction to staff. Provides technical support for secure software development and integration tasks, including reviewing work products for correctness and adhering to the design concept and to user standards. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Coordinates with system and network owners to cooperatively review architectures and provide advisement on vulnerabilities with associated remediation recommendations. Knowledgeable of Security/Information Assurance (IA) products such as PKI, VPN, firewalls, and intrusion detection systems. Analyzes and recommends resolution of security/IA problems on the basis of knowledge of the major IA products and services, an understanding of their limitations, and knowledge of the IA disciplines.</p> <p>Provides daily supervision and direction to staff when leading a team.</p>	<p>6 years</p>	<p>Bachelor's degree in a related field or security certification (CCIE, LPT, or CISSP)</p>

<p>141. RVA- Cyber Information Assurance Specialist I</p>	<p>Under specific guidance, performs technical support focused on the development, operation, management, and enforcement of cybersecurity capabilities for systems and networks. Cybersecurity support is concentrated on the protection and defense of information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for their restoration by incorporating protection, detection, and reaction capabilities. Supports or conducts authorized penetration testing on systems and networks. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Coordinates with system and network owners to cooperatively review architectures and provide advisement on vulnerabilities with associated remediation recommendations</p>	<p>2 years</p>	<p>At least 60 semester hours of education in a related field and a technical certification listed in DoD 8570.01 IAT level I or DoD 8570.01 IAM level I requirement</p>
<p>142. RVA- Cyber Information Assurance Specialist II</p>	<p>Under general supervision, performs technical support focused on the development, operation, management, and enforcement of cybersecurity capabilities for systems and networks. Cybersecurity support is concentrated on the protection and defense of information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for their restoration by incorporating protection, detection, and reaction capabilities. Supports or conducts authorized penetration testing on systems and networks. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Coordinates with system and network owners to cooperatively review architectures and provide advisement on vulnerabilities with associated remediation recommendations.</p>	<p>2 years</p>	<p>At least 60 semester hours of education in a related field and a technical certification listed in DoD 8570.01 IAT level II or DoD 8570.01 IAM level II requirements</p>

<p>143. RVA- Cyber Information Assurance Specialist III</p>	<p>Works independently or manages a team of security engineers to apply advanced security knowledge to programs. Performs technical support focused on the development, operation, management, and enforcement of cybersecurity capabilities for systems and networks.</p> <p>Cybersecurity support is concentrated on the protection and defense of information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for their restoration by incorporating protection, detection, and reaction capabilities. Supports or conducts authorized penetration testing on systems and networks. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Coordinates with system and network owners to cooperatively review architectures and provide advisement on vulnerabilities with associated remediation recommendations.</p>	<p>6 years</p>	<p>Bachelor's degree in a related field and a technical certification listed in DoD 8570.01 IAT level II or DoD 8570.01 IAM level II requirements</p>
<p>144. RVA- Cybersecurity Consultant I</p>	<p>Experience with several ADP architectures and platforms in an integrated environment. Stays current with advances in information technology. Assists in the analysis of current and projected service maintenance personnel and facility requirements. Designs interfaces to allow incompatible equipment to function as a unified system.</p>	<p>3 years</p>	<p>Bachelor's degree in a related field</p>

<p>145. RVA-Cybersecurity Consultant II</p>	<p>Leads major portions of large or medium projects and leads small projects autonomously. Gathers facts through research, interviewing, surveys, etc. Analyzes the client's business, draws conclusions, prepares final reports and gives presentations. Uses in-depth consultative skills and business knowledge to practice business objectives and processes. Manages and implements large, complex information technology systems. Advises senior executives on effective utilization of information technology systems and reengineering to meet business objectives. Identifies user requirements and describes services available or refers inquiries to other staff within installation. Provides technical support of a limited scope to users and assists them in defining and solving computing problems within well-defined areas of responsibility. Assists in preparing documentation of supported products for other staff members and users. Assists in preparing user training materials and conduct training sessions as assigned. Performs programming tasks of limited scope to assist users.</p>	<p>4 years</p>	<p>Bachelor's degree in a related field</p>
<p>146. RVA-Cybersecurity Consultant III</p>	<p>Manages the project work as defined by the client contract. Leads medium to large complex projects and major phases of very large projects. Manages the fact-finding, analysis, and development of hypothesis/conclusions, production of final reports, and delivery of presentations. Ensures that the project delivers to client expectations on time and to budget.</p>	<p>6 years</p>	<p>Bachelor's degree in a related field</p>
<p>147. RVA-Cybersecurity Consultant IV</p>	<p>Manages and implements large, complex information technology systems. Experienced in advising senior executives on effective utilization of information technology systems and reengineering to meet business objectives. Identifies user requirements and describes services available or refers inquiries to other staff within installation. Provides technical support of a limited scope to users and assists them in defining and solving computing problems within well-defined areas of responsibility. Assists in preparing documentation of supported products for other staff members and users. Assists in preparing user training materials and conducts training sessions as assigned. Performs programming tasks of limited scope to assist users.</p>	<p>6 years</p>	<p>Master's degree in a related field</p>

<p>148. RVA-Cybersecurity Consultant V</p>	<p>Serves as a Management Information System (MIS) manager. Designs, develops and manages implementation of risk assessment and business contingency planning framework, methodology, and tools to ensure business continuity of operations across a large, multi-division, decentralized organization. Supports multi-language, multi-platform and multi-operating system operations and utilizes electronic commerce and Electronic Data Interchange (EDI) applications. Recognizes and recommends new or emerging technology or software to satisfy functional requirements and processes. Provides highly technical and/or specialized guidance concerning automation solutions to complex information processing problems related to the subject field. Provides customer support using enterprise solutions software to integrate business areas consistent with today's technology in order to operate in an open systems environment and client service architecture. Analyzes data processing requirements to plan EDP systems to provide system capabilities required for projected workloads. Plans layout and installation of new systems or modification of existing systems. May set up and control analog or hybrid computer systems to solve scientific and engineering problems. Knowledgeable in Oracle, Windows NT, network administration, project management and Unix and Cobol programming. Internet Development/Integration. Develops applications that take advantage of Internet protocols and platforms. Internet developers extend beyond traditional software development disciplines to demonstrate advanced graphical design abilities, familiarity with new media formats, and solid understanding of Internet communications protocols and services. Deploys new applications that utilize Internet standards to enable wide access from the diverse client types found throughout the public Internet</p>	<p>8 years</p>	<p>Master's degree in a related field</p>
--	--	----------------	---

<p>149. RVA-Cybersecurity Consultant VI</p>	<p>Senior consultant to top level management. Viewed as the expert in discipline or related area of expertise, exhibiting an exceptional degree of ingenuity, creativity, and resourcefulness. Managerial/leadership experience required. Typically serves as the prime spokesperson to the customer. Performs technical planning, system integration, verification and validation, cost and risk, and supportability and effectiveness analyses for total systems. Analyses are performed at all levels of total system product to include: hardware/software, concept, design, fabrication, test, installation, operation, maintenance, and disposal. Performs duties such as site surveys, system evaluation, system analysis, architecture, and infrastructure assessment. Ensures the logical and systematic conversion of customer or product requirements into total systems solutions that acknowledge technical, schedule, and cost constraints. Applies and/or develops advanced technologies, scientific principles, theories, and concepts. Often acts independently to resolve issues associated with the development and implementation of operational programs. Plans R&amp;D programs and recommends technological application programs to accomplish long-range objectives</p>	<p>10 years</p>	<p>Master's degree in a related field</p>
---	---	-----------------	---

<p>150. RVA- Cyberspace Program Manager</p>	<p>Serves as the contractor’s single contract manager and shall be the contractor’s authorized interface with the Government Contracting Officer (CO), Government management personnel and customer agency representatives. Coordinates authorized penetration testing on systems and networks. Leads command and control functions in response to incidents. Supervises the collection of intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Oversees the coordination of incident data to identify specific vulnerabilities and recommends remediation actions. Manages teams and provides quality assurance with vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Responsible for formulating and enforcing work standards, assigning contractor schedules, reviewing work discrepancies, supervising contractor personnel and communicating policies, purposes, and goals of the organization to subordinates.</p>	<p>6 years</p>	<p>Bachelor’s degree in a related field, PMP certification</p>
<p>151. RVA- Risk and Vulnerability Analyst I</p>	<p>Supports the identification, assessment, and prioritization of risks followed by the coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. Supports all aspects of the Risk Management Framework to include categorize, select, implement, assess, authorize, and monitor security controls. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Coordinates with system and network owners</p>	<p>1 year</p>	<p>Associates degree in a related field</p>

	<p>to cooperatively review architectures and provide advisement on vulnerabilities with associated remediation recommendations. Supports the systematic examination of information systems and networks to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation</p>		
<p>152. RVA- Risk and Vulnerability Analyst II</p>	<p>Supports the identification, assessment, and prioritization of risks followed by the coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. Supports all aspects of the Risk Management Framework to include categorize, select, implement, assess, authorize, and monitor security controls. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Coordinates with system and network owners to cooperatively review architectures and provide advisement on vulnerabilities with associated remediation recommendations. Supports the systematic examination of information systems and networks to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation.</p>	<p>4 years</p>	<p>Bachelor's degree in a related field</p>

<p>153. RVA- Risk and Vulnerability Analyst III</p>	<p>Supports the identification, assessment, and prioritization of risks followed by the coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. Supports all aspects of the Risk Management Framework to include categorize, select, implement, assess, authorize, and monitor security controls. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Coordinates with system and network owners to cooperatively review architectures and provide advisement on vulnerabilities with associated remediation recommendations. Supports the systematic examination of information systems and networks to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation</p>	<p>6 years</p>	<p>Bachelor's degree in a related field</p>
<p>154. RVA- Risk and Vulnerability Analyst IV</p>	<p>Supports the identification, assessment, and prioritization of risks followed by the coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. Supports all aspects of the Risk Management Framework to include categorize, select, implement, assess, authorize, and monitor security controls. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Coordinates with system and network owners to cooperatively review architectures and provide advisement on vulnerabilities with associated remediation recommendations. Supports the systematic examination of information systems and networks to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.</p>	<p>6 years of relevant experience</p>	<p>Master's degree in a related field</p>

<p>155. RVA- Risk and Vulnerability Analyst V</p>	<p>Supports the identification, assessment, and prioritization of risks followed by the coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. Supports all aspects of the Risk Management Framework to include categorize, select, implement, assess, authorize, and monitor security controls. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Coordinates with system and network owners to cooperatively review architectures and provide advisement on vulnerabilities with associated remediation recommendations. Supports the systematic examination of information systems and networks to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation.</p>	<p>8 years</p>	<p>Master's degree in a related field</p>
<p>156. RVA- Cybersecurity Subject Matter Expert I</p>	<p>Under broad direction, provides support, analysis, and research into complex problems and processes relating to the subject matter. Serves as technical advisor on high-level project teams providing technical direction, interpretation, and alternatives. Thinks independently and demonstrates superior written and oral communications skills. Possesses a complete understanding and wide experience in the application of technical principles, theories, and concepts in the field. Provides technical solutions to a wide range of difficult problems. Solutions are imaginative, thorough, practicable, and consistent with organizational objectives. Independently determines and develops approach to solutions. Contributes to the completion of specific programs and projects. Possesses expertise in a particular area of Information Technology (e.g., Penetration Testing, Incident Response, Cyber Hunt, Risk and Vulnerability Assessments).</p>	<p>4 years</p>	<p>Bachelor's Degree in a related field</p>

<p>157. RVA-Cybersecurity Subject Matter Expert II</p>	<p>With minimal direction, provides Intermediate level support, analysis, and research into exceptionally complex problems and processes relating to the subject matter. Serves as technical expert on executive-level project teams providing technical direction, interpretation and alternatives. Thinks independently and demonstrates exceptional written and oral communications skills. Applies extensive technical expertise, 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. Exercises considerable latitude in determining technical objectives of assignment. Possesses expertise in a particular area of Information Technology (e.g., Penetration Testing, Incident Response, Cyber Hunt, Risk and Vulnerability Assessments).</p>	<p>6 years of relevant experience</p>	<p>Bachelor's degree in a related field</p>
<p>158. RVA-Cybersecurity Subject Matter Expert III</p>	<p>Provides expert support, analysis, and research into exceptionally complex problems, and processes relating to the subject matter. Serves as technical expert on executive-level project teams providing technical direction, interpretation and alternatives. Thinks independently and demonstrates exceptional written and oral communications skills. Applies advanced technical principles, theories, and concepts. Contributes to the development of new principles and concepts. Works on unusually complex technical problems and provides solutions which are highly innovative. Works under consultative direction toward predetermined long-range goals and objectives. Assignments are often self-initiated. Determines and pursues courses of action necessary to obtain desired results. Develops advanced technological ideas and guides their development into a final product. Possesses expertise in a particular area of Information Technology (e.g., Penetration Testing, Incident Response, Cyber Hunt, Risk and Vulnerability Assessments).</p>	<p>4 years</p>	<p>Master's degree in a related field</p>

<p>159. RVA-Cybersecurity Subject Matter Expert IV</p>	<p>Provides architecture and engineering SME support across multiple enterprise level initiatives. Determines and identifies high-level functional and technical requirements based on interactions with the user community and knowledge of the existing enterprise architecture. Designs enterprise architectures to include the software, hardware and communications to support the enterprise requirements as well as provide for present and future cross-functional requirements and interfaces. Identifies, assesses, and presents options for meeting the functional and technical requirements including hardware and software updates or upgrades. Develops high-level system design diagrams. Ensures systems are compatible and in compliance with the standards for open systems architectures, the Open Systems Interconnection (OSI) and International Standards Organization (ISO) reference models, and profiles of standards. Ensures compliance with standards and directives. Evaluates problems of work flows, organization and planning and develops appropriate corrective action. Evaluates and recommends new technologies.</p>	<p>6 years</p>	<p>Master's degree in a related field</p>
<p>160. RVA-Cybersecurity Training Specialist I</p>	<p>Under specific guidance, develops, plans, coordinates, delivers, and/or evaluates instructional cybersecurity content using various training methods, tactics, tools, and techniques. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments.</p>	<p>0 years</p>	<p>Associate's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCNA or CEH)</p>

<p>161. RVA-Cybersecurity Training Specialist II</p>	<p>Under general supervision, develops, plans, coordinates, delivers, and/or evaluates instructional cybersecurity content using various training methods, tactics, tools, and techniques. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments.</p>	<p>3 years</p>	<p>Associate's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCNA or CEH)</p>
<p>162. RVA-Cybersecurity Training Specialist III</p>	<p>Develops, plans, coordinates, delivers, and/or evaluates instructional cybersecurity content using various training methods, tactics, tools, and techniques. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Provides daily supervision and direction to staff when leading a team.</p>	<p>6 years</p>	<p>Bachelor's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCNA or ECSA)</p>

<p>163. RVA-Cybersecurity Training Specialist IV</p>	<p>Provides expertise in cybersecurity training discipline or related area of expertise, exhibiting an exceptional degree of ingenuity, creativity, and resourcefulness. Develops, plans, coordinates, delivers, and/or evaluates instructional cybersecurity content using various training methods, tactics, tools, and techniques. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments.</p>	<p>12 years</p>	<p>Master’s degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCIE, LPT, or CISSP)</p>
<p>164. RVA-Cybersecurity Training Specialist V</p>	<p>Serves as the onsite Training team lead. Designs, develops and manages implementation of cybersecurity training curriculum and materials. Senior consultant to top level management. Viewed as the expert in cybersecurity training discipline or related area of expertise, exhibiting an exceptional degree of ingenuity, creativity, and resourcefulness. Develops, plans, coordinates, delivers, and/or evaluates instructional cybersecurity content using various training methods, tactics, tools, and techniques. Analyzes CND policies or configurations and evaluates compliance with enterprise directives and regulations. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments.</p>	<p>14 years</p>	<p>Master’s degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCIE, LPT, or CISSP)</p>

<p>165. RVA- Cyber Threat Analyst I</p>	<p>Under specific guidance, conducts all–source analysis, digital forensics, and targeting to identify, monitor, assess, and counter the threat posed by foreign cyber actors against information systems, critical infrastructure and cyber–related interests. Produces strategic assessments and provide tactical analysis and advice for cyber and intelligence operations. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Applies scientific and technical knowledge to solve complex cyber and intelligence problems, produces short–term and long–term written assessments, and briefs decision makers to support organizational risk decision making.</p>	<p>0 years</p>	<p>Associate’s degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or rsecurity certification (CCNA or CEH)</p>
<p>166. RVA- Cyber Threat Analyst II</p>	<p>Under general supervision, conducts all–source analysis, digital forensics, and targeting to identify, monitor, assess, and counter the threat posed by foreign cyber actors against information systems, critical infrastructure and cyber–related interests. Produces strategic assessments and provide tactical analysis and advice for cyber and intelligence</p>	<p>3 years</p>	<p>Associate’s degree in Computer Science, Physics, Mathematics,</p>

	<p>operations. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Applies scientific and technical knowledge to solve complex cyber and intelligence problems, produces short-term and long-term written assessments, and briefs decision makers to support organizational risk decision making.</p>		<p>Operations Research, Information Technology, or security certification (CCNA or CEH)</p>
<p>167. RVA- Cyber Threat Analyst III</p>	<p>Conducts all-source analysis, digital forensics, and targeting to identify, monitor, assess, and counter the threat posed by foreign cyber actors against information systems, critical infrastructure and cyber-related interests. Produces strategic assessments and provide tactical analysis and advice for cyber and intelligence operations. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Applies scientific and technical knowledge to solve complex cyber and intelligence problems, produces short-term and long-term written assessments, and briefs decision makers to support organizational risk decision making.</p>	<p>6 years</p>	<p>Bachelor's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCNA or ECSCA)</p>

<p>168. RVA- Cyber Threat Analyst IV</p>	<p>Provides expertise in cyber threat analysis discipline or related area of expertise, exhibiting an exceptional degree of ingenuity, creativity, and resourcefulness. Conducts all-source analysis, digital forensics, and targeting to identify, monitor, assess, and counter the threat posed by foreign cyber actors against information systems, critical infrastructure and cyber-related interests. Produces strategic assessments and provide tactical analysis and advice for cyber and intelligence operations. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents.</p> <p>Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Applies scientific and technical knowledge to solve complex cyber and intelligence problems, produces short-term and long-term written assessments, and briefs decision makers to support organizational risk decision making.</p>	<p>12 years</p>	<p>Master's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCIE, LPT, or CISSP)</p>
--	---	-----------------	--

<p>169. RVA-Defensive Cyberspace Operator I</p>	<p>Under specific guidance, supports activities to defend friendly cyberspace. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Performs internal defensive measures to include actively hunting for advanced internal threats as well as the internal responses to these threats. Responds to unauthorized activity or alerts/threat information, and leverages intelligence, and other capabilities as required. Performs technical and non-technical activities and actions to protect, monitor, analyze, detect, and respond to unauthorized activity within information systems and networks. Supports passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems</p>	<p>0 years</p>	<p>Associate's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCNA or CEH)</p>
---	--	----------------	---

<p>170. RVA-Defensive Cyberspace Operator II</p>	<p>Under general supervision, supports activities to defend friendly cyberspace. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Performs internal defensive measures to include actively hunting for advanced internal threats as well as the internal responses to these threats. Responds to unauthorized activity or alerts/threat information, and leverages intelligence, and other capabilities as required. Performs technical and non- technical activities and actions to protect, monitor, analyze, detect, and respond to unauthorized activity within information systems and networks. Supports passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.</p>	<p>3 years</p>	<p>Associate's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCNA or ECSA)</p>
<p>171. RVA-Defensive Cyberspace Operator III</p>	<p>Supports activities to defend friendly cyberspace. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Performs internal defensive measures to include actively hunting for</p>	<p>6 years</p>	<p>Bachelor's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification</p>

	<p>advanced internal threats as well as the internal responses to these threats. Responds to unauthorized activity or alerts/threat information, and leverages intelligence, and other capabilities as required. Performs technical and non-technical activities and actions to protect, monitor, analyze, detect, and respond to unauthorized activity within information systems and networks. Supports passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.</p>		(CCIE, LPT, or CISSP)
172. RVA-Defensive Cyberspace Operator IV	<p>Provides expertise in defensive cyber operations discipline or related area of expertise, exhibiting an exceptional degree of ingenuity, creativity, and resourcefulness. Supports activities to defend friendly cyberspace. Supports or conducts authorized penetration testing on systems and networks. Conducts command and control functions in response to incidents. Collects intrusion artifacts and conducts analysis to support the mitigation of potential threats. Supports CND Technicians with coordination support, data correlation and threat identification attribution of CND incidents. Correlates incident data to identify specific vulnerabilities and recommends remediation actions. Conducts vulnerability scanning, network mapping, wireless network assessments, web application assessments, and network perimeter protection assessments. Performs internal defensive measures to include actively hunting for advanced internal threats as well as the internal responses to these threats. Responds to unauthorized activity or alerts/threat information, and leverages intelligence, and other capabilities as required. Performs technical and non-technical activities and actions to protect, monitor, analyze, detect, and respond to unauthorized activity within information systems and networks. Supports passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.</p>	10 years	Bachelor's degree in Computer Science, Physics, Mathematics, Operations Research, Information Technology, or security certification (CCIE, LPT, or CISSP)

Sealing Technologies, Inc. will provide people who meet or exceed the minimum qualifications within the labor category descriptions stated herein. Sealing Tech labor categories provide for substituting experience for minimum education requirements and substituting educational degrees for years of experience. These substitutions are allowed for all Sealing Tech labor categories unless specified in the description.

**ALLOWABLE SUBSTITUTIONS**

In general, where it is not stated, the following experience table may be substituted for not having the required degree, unless otherwise specified in the job description. The table below presents the allowable substitutions based on the education and experience of the labor categories in the Pricelist. Experience should be professional, and job related, however it does not have to be specific to the project to be accomplished.

<b>Degree</b>	<b>Degree, Experience, and Education Substitutions</b>	<b>Related Certification Substitutions</b>
Associate's	2 years relevant experience	Trade school, vocational school, technical training, or military training in a relevant field.
Bachelor's	Associate's + 4 years relevant experience 6 years relevant experience	Professional or industry standard technical certification in a relevant field.
Master's	Bachelor's + 4 years relevant experience Associate's + 8 years relevant experience 10 years relevant experience	Professional license in a relevant field.
Doctorate	Master's + 4 years relevant experience Bachelor's + 8 years relevant experience 14 years relevant experience	

## Pricing

### LABOR CATEGORIES

SIN	Labor Category	GSA Price with IFF	
		Gov. Site	Cont. Site
54151S	Network Systems Engineer I	\$56.82	\$62.09
54151S	Network Systems Engineer II	\$69.61	\$75.49
54151S	Network Systems Engineer III	\$82.84	\$89.84
54151S	Technical Writer/Editor II	\$56.04	\$60.78
54151S	Technical Writer/Editor III	\$74.05	\$80.31
54151S	Functional Analyst I	\$62.05	\$67.29
54151S	Functional Analyst II	\$80.06	\$86.83
54151S	Information Systems Security Specialist I	\$74.08	\$80.34
54151S	Information Systems Security Specialist II	\$89.40	\$96.96
54151S	Information/Computer/Telecommunications I	\$72.17	\$78.28
54151S	Information/Computer/Telecommunications II	\$86.60	\$93.92
54151S	Information/Computer/Telecommunications III	\$101.84	\$110.45
54151S	Information Assurance Specialist I	\$65.27	\$70.79
54151S	Information Assurance Specialist II	\$80.64	\$87.46
54151S	Information Assurance Specialist III	\$114.33	\$123.99
54151S	Systems Engineer I	\$67.97	\$73.71
54151S	Systems Engineer II	\$95.48	\$103.55
54151S	Systems Engineer III	\$113.34	\$122.92
54151S	Systems Administrator I	\$80.41	\$87.20

SIN	Labor Category	GSA Price with IFF	
		Gov. Site	Cont. Site
54151S	Systems Administrator II	\$95.96	\$104.07
54151S	Systems Administrator III	\$106.56	\$115.57
54151S	Network Design Engineer I	\$66.80	\$72.45
54151S	Network Design Engineer II	\$102.61	\$111.29
54151S	Network Design Engineer III	\$121.17	\$131.42
54151S	Consultant I	\$75.05	\$81.40
54151S	Consultant II	\$100.08	\$108.53
54151S	Consultant III	\$125.09	\$135.67
54151S	Business Process Engineer I	\$92.47	\$100.29
54151S	Business Process Engineer II	\$114.85	\$124.55
54151S	Business Process Engineer III	\$126.63	\$137.33
54151S	Computer Security Systems Specialist I	\$100.08	\$108.53
54151S	Computer Security Systems Specialist II	\$150.11	\$162.80
54151S	Computer Security Systems Specialist III	\$200.15	\$217.07
54151S	Operations Manager	\$80.06	\$86.83
54151S	Program Manager	\$150.11	\$162.80
54151S	Subject Matter Expert I	\$96.07	\$104.19
54151S	Subject Matter Expert II	\$110.08	\$119.39
54151S	Subject Matter Expert III	\$122.09	\$132.41
54151S	Subject Matter Expert IV	\$150.11	\$162.80
54151S	Systems Architect III	\$119.35	\$129.44
54151S	Systems Architect IV	\$141.68	\$153.65

SIN	Labor Category	GSA Price with IFF	
		Gov. Site	Cont. Site
54151S	Software Developer I	\$150.11	\$162.80
54151S	Software Developer II	\$175.13	\$189.93
54151S	Software Developer III	\$200.15	\$217.07
54151S	Information Technology Consultant I	\$67.05	\$72.72
54151S	Information Technology Consultant II	\$75.05	\$81.40
54151S	Information Technology Consultant III	\$100.08	\$108.53
54151S	Information Technology Consultant IV	\$138.11	\$149.78
54151S	Information Technology Consultant V	\$175.13	\$189.93
54151S	Information Technology Consultant VI	\$252.19	\$273.51
ANCILLARY	Program Administration Specialist	\$65.05	\$70.55
ANCILLARY	Quality Assurance Analyst	\$95.07	\$103.11
ANCILLARY	Project Manager	\$112.08	\$121.56
ANCILLARY	Task Order Manager	\$125.09	\$135.67
ANCILLARY	Quality Assurance Manager	\$140.11	\$151.95
SIN	Labor Category	GSA Price with IFF	
		Cont. Site	Govt. Site
54151HACS	PT Cyber Information Assurance Specialist I	\$75.16	\$68.40
54151HACS	PT Cyber Information Assurance Specialist II	\$92.86	\$84.50
54151HACS	PT Cyber Information Assurance Specialist III	\$131.63	\$119.78
54151HACS	PT Computer Security Systems Specialist I	\$115.23	\$104.86
54151HACS	PT Computer Security Systems Specialist II	\$172.85	\$157.29

SIN	Labor Category	GSA Price with IFF	
		Cont. Site	Gov. Site
54151HACS	PT Computer Security Systems Specialist III	\$230.45	\$209.71
54151HACS	PT Cyberspace Program Manager	\$172.85	\$157.29
54151HACS	PT Cybersecurity Subject Matter Expert I	\$110.62	\$100.66
54151HACS	PT Cybersecurity Subject Matter Expert II	\$126.74	\$115.33
54151HACS	PT Cybersecurity Subject Matter Expert III	\$140.57	\$127.92
54151HACS	PT Cybersecurity Subject Matter Expert IV	\$172.85	\$157.29
54151HACS	PT Cybersecurity Consultant I	\$77.21	\$70.26
54151HACS	PT Cybersecurity Consultant II	\$86.43	\$78.65
54151HACS	PT Cybersecurity Consultant III	\$115.23	\$104.86
54151HACS	PT Cybersecurity Consultant IV	\$159.01	\$144.70
54151HACS	PT Cybersecurity Consultant V	\$201.65	\$183.50
54151HACS	PT Cybersecurity Consultant VI	\$290.38	\$264.25
54151HACS	PT Cyber Threat Analyst I	\$90.39	\$82.25
54151HACS	PT Cyber Threat Analyst II	\$105.50	\$96.01
54151HACS	PT Cyber Threat Analyst III	\$120.61	\$109.76
54151HACS	PT Cyber Threat Analyst IV	\$135.69	\$123.48
54151HACS	PT Defensive Cyberspace Operator I	\$77.08	\$70.14
54151HACS	PT Defensive Cyberspace Operators II	\$93.18	\$84.79
54151HACS	PT Defensive Cyberspace Operator III	\$109.28	\$99.44
54151HACS	PT Defensive Cyberspace Operator IV	\$125.37	\$114.09

SIN	Labor Category	GSA Price with IFF	
		Cont. Site	Gov. Site
54151HACS	PT Offensive Cyberspace Operator I	\$80.37	\$73.14
54151HACS	PT Offensive Cyberspace Operator II	\$96.48	\$87.80
54151HACS	PT Offensive Cyberspace Operator III	\$112.57	\$102.44
54151HACS	PT Offensive Cyberspace Operator IV	\$128.68	\$117.10
54151HACS	PT Cybersecurity Training Specialist I	\$97.16	\$88.42
54151HACS	PT Cybersecurity Training Specialist II	\$113.41	\$103.20
54151HACS	PT Cybersecurity Training Specialist III	\$129.66	\$117.99
54151HACS	PT Cybersecurity Training Specialist IV	\$145.87	\$132.74
54151HACS	PT Cybersecurity Training Specialist V	\$166.62	\$151.62
54151HACS	IR Computer Security Systems Specialist I	\$115.23	\$104.86
54151HACS	IR Computer Security Systems Specialist II	\$172.85	\$157.29
54151HACS	IR Computer Security Systems Specialist III	\$230.45	\$209.71
54151HACS	IR Cyberspace Program Manager	\$172.85	\$157.29
54151HACS	IR Cybersecurity Subject Matter Expert I	\$110.62	\$100.66
54151HACS	IR Cybersecurity Subject Matter Expert II	\$126.74	\$115.33
54151HACS	IR Cybersecurity Subject Matter Expert III	\$140.57	\$127.92
54151HACS	IR Cybersecurity Subject Matter Expert IV	\$172.85	\$157.29
54151HACS	IR Cybersecurity Consultant I	\$77.21	\$70.26
54151HACS	IR Cybersecurity Consultant II	\$86.43	\$78.65
54151HACS	IR Cybersecurity Consultant III	\$115.23	\$104.86

SIN	Labor Category	GSA Price with IFF	
		Cont. Site	Gov. Site
54151HACS	IR Cybersecurity Consultant IV	\$159.01	\$144.70
54151HACS	IR Cybersecurity Consultant V	\$201.65	\$183.50
54151HACS	IR Cybersecurity Consultant VI	\$290.38	\$264.25
54151HACS	IR Cyber Threat Analyst I	\$90.39	\$82.25
54151HACS	IR Cyber Threat Analyst II	\$105.50	\$96.01
54151HACS	IR Cyber Threat Analyst III	\$120.61	\$109.76
54151HACS	IR Cyber Threat Analyst IV	\$135.69	\$123.48
54151HACS	IR Defensive Cyberspace Operations I	\$77.08	\$70.14
54151HACS	IR Defensive Cyberspace Operations II	\$93.18	\$84.79
54151HACS	IR Defensive Cyberspace Operations III	\$109.28	\$99.44
54151HACS	IR Defensive Cyberspace Operations IV	\$125.37	\$114.09
54151HACS	CH Computer Security Systems Specialist I	\$115.23	\$104.86
54151HACS	CH Computer Security Systems Specialist II	\$172.85	\$157.29
54151HACS	CH Computer Security Systems Specialist III	\$230.45	\$209.71
54151HACS	CH Cyberspace Program Manager	\$172.85	\$157.29
54151HACS	CH Cybersecurity Subject Matter Expert I	\$110.62	\$100.66
54151HACS	CH Cybersecurity Subject Matter Expert II	\$126.74	\$115.33
54151HACS	CH Cybersecurity Subject Matter Expert III	\$140.57	\$127.92
54151HACS	CH Cybersecurity Subject Matter Expert IV	\$172.85	\$157.29
54151HACS	CH Cybersecurity Consultant I	\$77.21	\$70.26

SIN	Labor Category	GSA Price with IFF	
		Cont. Site	Gov. Site
54151HACS	CH Cybersecurity Consultant II	\$86.43	\$78.65
54151HACS	CH Cybersecurity Consultant III	\$115.23	\$104.86
54151HACS	CH Cybersecurity Consultant IV	\$159.01	\$144.70
54151HACS	CH Cybersecurity Consultant V	\$201.65	\$183.50
54151HACS	CH Cybersecurity Consultant VI	\$290.38	\$264.25
54151HACS	CH Cyber Threat Analyst I	\$90.39	\$82.25
54151HACS	CH Cyber Threat Analyst II	\$105.50	\$96.01
54151HACS	CH Cyber Threat Analyst III	\$120.61	\$109.76
54151HACS	CH Cyber Threat Analyst IV	\$135.69	\$123.48
54151HACS	CH Offensive Cyberspace Operator I	\$80.37	\$73.14
54151HACS	CH Offensive Cyberspace Operator II	\$96.48	\$87.80
54151HACS	CH Offensive Cyberspace Operator III	\$112.57	\$102.44
54151HACS	CH Offensive Cyberspace Operator IV	\$128.68	\$117.10
54151HACS	CH Defensive Cyberspace Operator I	\$77.08	\$ 70.14
54151HACS	CH Defensive Cyberspace Operator II	\$96.14	\$87.49
54151HACS	CH Defensive Cyberspace Operator III	\$109.28	\$99.44
54151HACS	CH Defensive Cyberspace Operator IV	\$125.37	\$114.09
54151HACS	RAV Cyber Information Assurance Specialist I	\$75.16	\$68.40
54151HACS	RAV Cyber Information Assurance Specialist II	\$92.86	\$84.50
54151HACS	RAV Cyber Information Assurance Specialist III	\$131.63	\$119.78

SIN	Labor Category	GSA Price with IFF	
		Cont. Site	Gov. Site
54151HACS	RAV Computer Security Systems Specialist I	\$115.23	\$104.86
54151HACS	RAV Computer Security Systems Specialist II	\$172.85	\$157.29
54151HACS	RAV Computer Security Systems Specialist III	\$230.45	\$209.71
54151HACS	RAV Cyberspace Program Manager	\$172.85	\$157.29
54151HACS	RAV Cybersecurity Subject Matter Expert I	\$110.62	\$100.66
54151HACS	RAV Cybersecurity Subject Matter Expert II	\$126.74	\$115.33
54151HACS	RAV Cybersecurity Subject Matter Expert III	\$140.57	\$127.92
54151HACS	RAV Cybersecurity Subject Matter Expert IV	\$172.85	\$157.29
54151HACS	RAV Cybersecurity Consultant I	\$77.21	\$70.26
54151HACS	RAV Cybersecurity Consultant II	\$86.43	\$78.65
54151HACS	RAV Cybersecurity Consultant III	\$115.23	\$104.86
54151HACS	RAV Cybersecurity Consultant IV	\$159.01	\$144.70
54151HACS	RAV Cybersecurity Consultant V	\$201.65	\$183.50
54151HACS	RAV Cybersecurity Consultant VI	\$290.38	\$264.25
54151HACS	RAV Cyber Threat Analyst I	\$90.39	\$82.25
54151HACS	RAV Cyber Threat Analyst II	\$105.50	\$96.01
54151HACS	RAV Cyber Threat Analyst III	\$120.61	\$109.76
54151HACS	RAV Cyber Threat Analyst IV	\$135.69	\$123.48
54151HACS	RAV Defensive Cyberspace Operator I	\$77.08	\$70.14
54151HACS	RAV Defensive Cyberspace Operator II	\$93.18	\$84.79

SIN	Labor Category	GSA Price with IFF	
		Cont. Site	Gov. Site
54151HACS	RAV Defensive Cyberspace Operator III	\$109.28	\$ 9.44
54151HACS	RAV Defensive Cyberspace Operator IV	\$125.37	\$114.09
54151HACS	RAV Cybersecurity Training Specialist I	\$97.16	\$88.42
54151HACS	RAV Cybersecurity Training Specialist II	\$113.41	\$103.20
54151HACS	RAV Cybersecurity Training Specialist II	\$113.41	\$103.20
54151HACS	RAV Cybersecurity Training Specialist IV	\$145.87	\$132.74
54151HACS	RAV Cybersecurity Training Specialist V	\$166.62	\$151.62
54151HACS	RAV Risk and Vulnerability Analyst I	\$98.87	\$89.97
54151HACS	RAV Risk and Vulnerability Analyst II	\$116.37	\$105.90
54151HACS	RAV Risk and Vulnerability Analyst III	\$133.89	\$121.84
54151HACS	RAV Risk and Vulnerability Analyst IV	\$151.40	\$137.77
54151HACS	RAV Risk and Vulnerability Analyst V	\$171.52	\$156.08

## TRAINING

SIN	Course Title	Course Length	Minimum Participation	Maximum Participation	Price Offered to GSA (including IFF)
611420	SELinux Analysis	2.5 days	8 students	16 students	\$2,040.30per student + travel
<p>Two and Half (2.5) days of in-depth training on SELinux focusing on policy analysis for security-focused, information assurance systems including, specifically, cross-domain solutions (CDS). The class will include instructor lectures as well as hands-on activities for comprehension, providing example “real world” applications of the presented material. As part of the real world applications, Quark Security provides an example implementation of a file transfer cross-domain solution that will be analyzed during the hands-on portion of the training. In addition to lectures and hands-on exercises, this proposal includes delivery of all materials used including the slides used during the lectures and hands-on exercises as well as the virtual machines (VMs) used to analyze policies during the hands-on portions of the training.</p>					
611420	SELinux Development	2.5 days	8 students	16 students	\$2,040.30per student + travel
<p>Two and half days (2.5) days of in-depth training on SELinux focusing on policy development for security-focused, information assurance systems including, specifically, cross-domain solutions (CDS). The class will include instructor lectures as well as hands-on activities for comprehension, providing example “real world” applications of the presented material. As part of the real world applications, Quark Security provides an example implementation of a file transfer cross-domain solution that will be exercised and the SELinux policy will be developed during the hands-on portion of the training. In addition to lectures and hands-on exercises, this proposal includes delivery of all materials used including the slides used during the lectures and hands-on exercises as well as the virtual machines (VMs) used to analyze policies during the hands-on portions of the training.</p>					
611420	Bro	3 days	8 students	20 students	\$1,461.13 per student + travel
<p>The Bro IDS/Argus training course provides students with an overview of the Bro IDS and Argus programs. Students will receive hands on training with exercises in the lab paired with lecture to fully understand the products and their use. Upon completion of the course, student should have a working knowledge of Bro IDS/Argus and how to use both products in their environment. All attendees must have computer and internet access and all facilities must be provided by the customer.</p>					

SIN	MANUFACTURER NAME	PART NUMBER	PRODUCT DESCRIPTION	GSA PRICE	COO
33411	Sealing Technologies Incorporated	SN7064-SAS300	300TB SAS / 8TB M.2 / 512GB RAM	\$197,709.76	US
33411	Sealing Technologies Incorporated	SN7064-SAS240	240TB SAS / 8TB M.2 / 512GB RAM	\$169,977.00	US
33411	Sealing Technologies Incorporated	SN7064-SAS120	120TB SAS / 8TB M.2 / 512GB RAM	\$112,733.64	US
33411	Sealing Technologies Incorporated	SN7064-SAS60	60TB SAS / 2TB M.2 / 512GB RAM	\$85,001.79	US
33411	Sealing Technologies Incorporated	SN7064-SAS15	15TB SAS / 2TB M.2 / 512GB RAM	\$63,816.44	US
33411	Sealing Technologies Incorporated	SN7064-NVMe300	300TB U.2 NVMe / 8TB M.2 / 512GB RAM	\$253,451.27	US
33411	Sealing Technologies Incorporated	SN7064-NVMe240	240TB U.2 NVMe / 8TB M.2 / 512GB RAM	\$214,214.46	US
33411	Sealing Technologies Incorporated	SN7064-NVMe120	120TB U.2 NVMe / 8TB M.2 / 512GB RAM	\$135,741.74	US
33411	Sealing Technologies Incorporated	SN3016-SATA24	24TB SATA SSD, 256GB MEMORY	\$18,719.87	US
33411	Sealing Technologies Incorporated	SN3016-SATA8	8TB SATA SSD, 128GB MEMORY	\$11,400.44	US
33411	Sealing Technologies Incorporated	STCFLAK-SATA192	Sealing Tech C-FLAK Case (3), SN3016-SATA24 (8), SN4412 (1), SN4112 (1), A-Tap, Laptop	\$228,990.84	US
33411	Sealing Technologies Incorporated	STCFLAK-SATA64	Sealing Tech C-FLAK Case (3), SN3016-SATA8 (8), SN4412 (1), SN4112 (1), A-Tap, Laptop	\$170,434.52	US
511210	ShadowDragon Federal LLC	SD-FED-SocNet-250-MaltegoBundle	SocialNet Identity Management Secured Link Analysis Bundled With Maltego Classic - 250 Queries/Day - 12 Month Subscription	\$2,834.26	US
511210	ShadowDragon Federal LLC	SD-FED-SocNet-500-MaltegoBundle	SocialNet Identity Management Secured Link Analysis Bundled With Maltego Classic - 500 Queries/Day - 12 Month Subscription	\$4,202.52	US
511210	ShadowDragon Federal LLC	SD-FED-SocNet-1000-MaltegoBundle	SocialNet Identity Management Secured Link Analysis Bundled With Maltego Classic - 1000 Queries/Day - 12 Month Subscription	\$5,863.98	US
511210	ShadowDragon Federal LLC	SD-FED-SocNet-250-KasewareBundle	SocialNet Identity Management Secured Link Analysis Bundled With Kaseware Complete - 250 Queries/Day - 12 Month Subscription	\$3,127.46	US
511210	ShadowDragon Federal LLC	SD-FED-SocNet-500-KasewareBundle	SocialNet Identity Management Secured Link Analysis Bundled With Kaseware Complete - 500 Queries/Day - 12 Month Subscription	\$4,495.72	US
511210	ShadowDragon Federal LLC	SD-FED-SocNet-1000-KasewareBundle	SocialNet Identity Management Secured Link Analysis Bundled With Kaseware Complete - 1000 Queries/Day - 12 Month Subscription	\$6,157.18	US
511210	ShadowDragon Federal LLC	SD-FED-SocNet-250	SocialNet Identity Management Secured Link Analysis - 250 Queries/Day - 12 Month Subscription	\$1,368.26	US

# SEALINGTECH

Taking Cyber Security Seriously

SIN	MANUFACTURER NAME	PART NUMBER	PRODUCT DESCRIPTION	GSA PRICE	COO
511210	ShadowDragon Federal LLC	SD-FED-SocNet-500	SocialNet Identity Management Secured Link Analysis - 500 Queries/Day - 12 Month Subscription	\$2,736.52	US
511210	ShadowDragon Federal LLC	SD-FED-SocNet-1000	SocialNet Identity Management Secured Link Analysis - 1000 Queries/Day - 12 Month Subscription	\$4,397.98	US
511210	ShadowDragon Federal LLC	SD-FED-SocNetAPI-22	SocialNet API - 22 Queries/Hour - 12 Month Subscription	\$3,909.32	US
511210	ShadowDragon Federal LLC	SD-FED-SocNetAPI-42	SocialNet API - 42 Queries/Hour - 12 Month Subscription	\$4,691.18	US
511210	ShadowDragon Federal LLC	SD-FED-SocNetAPI-125	SocialNet API - 125 Queries/Hour - 12 Month Subscription	\$17,103.27	US
511210	ShadowDragon Federal LLC	SD-FED-SocNetAPI-250	SocialNet API - 250 Queries/Hour - 12 Month Subscription	\$34,206.55	US
511210	ShadowDragon Federal LLC	SD-FED-SocNetAPI-500	SocialNet API - 500 Queries/Hour - 12 Month Subscription	\$68,413.10	US
511210	ShadowDragon Federal LLC	SD-FED-SocNetAPI-1000	SocialNet API - 1000 Queries/Hour - 12 Month Subscription	\$136,826.20	US
511210	ShadowDragon Federal LLC	SD-SocNet-DEV-API	SocialNet Developer API Access for POC Integration - 1000 Queries/Day - 12 Month Subscription	\$6,352.64	US
511210	ShadowDragon Federal LLC	SD-FED-MalNet-1000	MalNet Consultant User License - 1000 Queries/Day - 12 Month Subscription	\$1,270.53	US
511210	ShadowDragon Federal LLC	SD-FED-MalNet-5000	MalNet Small Per User License - 5000 Queries/Day - 12 Month Subscription	\$5,082.12	US
511210	ShadowDragon Federal LLC	SD-FED-MalNet-25000	MalNet Medium Per User License - 25000 Queries/Day - 12 Month Subscription	\$9,362.82	US
511210	ShadowDragon Federal LLC	SD-FED-MalNet-UNLIM	MalNet Large Per User License - Unlimited Queries - 12 Month Subscription	\$13,975.82	US
511210	ShadowDragon Federal LLC	SD-FED-OIMon-API-1-User	OIMonitor Portal - SaaS Intelligence engine access + API Access - 1 user - 12 Month Subscription	\$38,115.87	US
511210	ShadowDragon Federal LLC	SD-FED-OIMon-UserAdd	OIMonitor Portal - SaaS Intelligence Engine Access, Additional User - 12 Month Subscription	\$3,909.32	US
511210	ShadowDragon Federal LLC	SD-FED-AliasDB-1000	AliasDB - 1000 Rate Limit - 1000 Per-Day - 12 Month Subscription	\$1,270.53	US
511210	ShadowDragon Federal LLC	SD-FED-AliasDB-5000	AliasDB - 5000 Rate Limit - 5000 Per-Day - 12 Month Subscription	\$5,082.12	US
511210	ShadowDragon Federal LLC	SD-FED-AliasDB-25000	AliasDB - 25000 Rate Limit - 25000 Per-Day - 12 Month Subscription	\$8,385.49	US
511210	ShadowDragon Federal LLC	SD-FED-AliasDB-API-42	AliasDB - API Access 42 Rate Limits - 42 Queries/Hour - 12 Month Subscription	\$1,465.99	US
511210	ShadowDragon Federal LLC	SD-FED-AliasDB-API-250	AliasDB - API Access 250 Rate Limit - 250 Queries/Hour - 12 Month Subscription	\$5,570.78	US

# SEALINGTECH

Taking Cyber Security Seriously

SIN	MANUFACTURER NAME	PART NUMBER	PRODUCT DESCRIPTION	GSA PRICE	COO
511210	ShadowDragon Federal LLC	SD-FED-AliasDB-API-1050	AliasDB - API Access 1050 Rate Limit - 1050 Queries/Hour - 12 Month Subscription	\$8,698.24	US
511210	ShadowDragon Federal LLC	SD-FED-AliasDB-API-UNLIM	AliasDB - API Access Unlimited Queries/Day - 12 Month Subscription	\$13,682.62	US
511210	ShadowDragon Federal LLC	SD-FED-SPOTTER	Spotter Targeting Appliance - Yearly Maintenance required - 12 Month Subscription	\$27,316.37	US
511210	ShadowDragon Federal LLC	SD-FED-SPOTTER-MAINT	Spotter Yearly Maintenance - 12 Month Subscription	\$4,097.94	US
511210	ShadowDragon Federal LLC	SD-FED-ConvertIT	ConvertIT Document Conversion Tool - 12 Month Subscription   3-year commitment	\$972.44	US
511210	ShadowDragon Federal LLC	SD-FED-ConvertIT-MAINT	ConvertIT Yearly Maintenance - 12 Month Subscription	\$1,089.72	US
511210	ShadowDragon Federal LLC	SD-Maltego-Classic	Maltego Classic License - Link Analysis to 10,000 Entities - 12 Month Subscription	\$1,465.99	US
511210	ShadowDragon Federal LLC	SD-Maltego-XL	Maltego XL License - Link Analysis to 1,000,000 Entities - 12 Month Subscription	\$2,931.99	US
511210	ShadowDragon Federal LLC	SD-Kaseware-Complete-Com	Kaseware Complete License (Commercial) - Link Analysis and Case Management - 12 Month Subscription	\$1,759.19	US
511210	ShadowDragon Federal LLC	SD-Kaseware-Complete-Gov	Kaseware Complete License (Commercial) - Link Analysis and Case Management - 12 Month Subscription	\$1,172.80	US
511210	ShadowDragon Federal LLC	SD-US-LEA-SocNet-Detective-Bundle	SocialNet + Kaseware Complete - 125 Queries/Day - 12 Month Subscription (APPROVE US Law Enforcement Agencies ONLY)	\$635.26	US
511210	ShadowDragon Federal LLC	SD-US-LEA-SocNet-ESSENTIALS-Training	SocialNet ESSENTIALS New User Training for US Law Enforcement Bundle (New User Training Required for LEA Bundle)   PER CLASS	\$1,465.99	US
511210	ShadowDragon Federal LLC	SD-FED-Bundle-ARCPlatform-AnalystKit	Bundle Kit for One Anaylst: *SocialNet+Maltego Classic Bundled License at 5000 Queries Per Day *Training Per Analyst Online or Onsite *Malnet License 5000 Queries Per Day *OIMonitor Platform License (1 OIMonitor User, Additional @ \$4000/user) * AliasDB Access 1000 Queries Per Day	\$48,768.77	US