

GENERAL SERVICES ADMINISTRATION Federal Supply Service

Authorized Federal Supply Service Pricelist

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 for GSA Advantage!® is: GSAAdvantage.gov.

GSA Multiple Award Schedule (MAS)

Contract Number: GS-35F-0032V

SIN 54151S (Information Technology Professional Services)
SIN 54151HACS (Highly Adaptive Cybersecurity Services)
SIN 518210C (Cloud Computing and Cloud Related IT Professional Services)
SIN ANCILLARY (Ancillary Supplies and Services)
SIN 511210 (Software Licenses)
SIN OLM (Order-Level Materials)

Contract Period: October 16, 2018 - October 15, 2023

Business Size: Large

Contract Director: Corionna Canada
corionna.canada@criterion-sys.com
703-942-5800 x351

Criterion Systems, Inc.
8330 Boone Blvd, Suite 400, Vienna, VA 22182
(703) 942-5800
(703) 942-5729 FAX
www.criterion-sys.com

Current through Modification PS-0034 dated December 17, 2021

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

Customer Information

1a. Table of awarded special item number(s) with appropriate cross-reference to item descriptions and awarded price(s).

Special Item Number	Special Item Description
54151S	Information Technology Professional Services
54151HACS	Highly Adaptive Cybersecurity Services (HACS)
518210C	Cloud Computing and Cloud Related IT Professional Services
ANCILLARY	Ancillary Supplies and Services
511210	Software Licenses
OLM	Order Level Materials

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 Pricing Below.

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. If hourly rates are not applicable, indicate "Not applicable" for this item.

See Pricing Below.

2. Maximum Order:

\$500,000

3. Minimum Order:

\$100.00

4. Geographic coverage (delivery area):

Worldwide

5. Point(s) of production (city, county, and State or foreign country):

Worldwide

6. Discount from list prices or statement of net price:

Prices shown are NET Prices; Basic discounts have been deducted.

7. Quantity Discounts:

None

-
8. Prompt payment terms:
0% - NET 30 days from receipt of invoice or date of acceptance, whichever is later. 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:
As negotiated with ordering activity.
- 10b. Expedited Delivery:
Contact contractor
- 10c. Overnight and 2-day delivery:
Contact contractor
- 10d. Urgent Requirements:
Ordering activities are encouraged to contact the contractor for purposes of obtaining accelerated delivery.
11. F.O.B Point(s):
Destination
- 12a. Ordering address(es):
**Criterion Systems, Inc.
8330 Boone Blvd, Suite 400
Vienna, Virginia 22182**
- 12b. Ordering procedures:
For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPAs) are found in Federal Acquisition Regulation (FAR) 8.405-3.
13. Payment address(es):
**Criterion Systems, Inc.
8330 Boone Blvd, Suite 400
Vienna, Virginia 22182**
Bank account information for EFT payments will be shown on the invoice
14. Warranty provision: **Not applicable**

15. Export packing charges, if applicable:

Not applicable

16. Terms and conditions of rental, maintenance, and repair (if applicable):

Not applicable

17. Terms and conditions of installation (if applicable):

Not applicable

18a. Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices (if applicable):

Not applicable

18b. Terms and conditions for any other services (if applicable):

Not applicable

19. List of service and distribution points (if applicable):

Not applicable

20. List of participating dealers (if applicable):

Not applicable

21. Preventive maintenance (if applicable):

Not applicable

22a. Special attributes such as environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants):

Not applicable

22b. If applicable, Section 508 compliance information is available on Electronic and Information Technology (EIT) supplies and services and show where full details can be found at www.criterion-sys.com. The EIT standards can be found at: www.Section508.gov/

23. Unique Entity Identifier (UEI) number:

MPGNDNHHWM33

24. Notification regarding registration in System for Award Management (SAM) database:
Criterion Systems, Inc. is registered in the System for Award Management database.

Terms and Conditions Applicable to Information Technology (IT) Professional Services (Special Item Number 54151S)

1. Scope
 - a. The prices, terms and conditions stated under Special Item Number 54151S Information Technology Professional Services exclusively to IT Services within the scope of this Multiple Award Schedule.
 - b. The Contractor shall provide services at the Contractor's facility and/or at the ordering activity location, as agreed to by the Contractor and the ordering activity.
2. Performance Incentives
 - a. Performance incentives may be agreed upon between the Contractor and the ordering activity on individual fixed price orders or Blanket Purchase Agreements under this contract in accordance with this clause.
 - b. The ordering activity must establish a maximum performance incentive price for these services and/or total solutions on individual orders or Blanket Purchase Agreements.
 - c. Incentives should be designed to relate results achieved by the contractor to specified targets. To the maximum extent practicable, ordering activities shall consider establishing incentives where performance is critical to the ordering activity's mission and incentives are likely to motivate the contractor. Incentives shall be based on objectively measurable tasks.
3. Order
 - a. Agencies may use written orders, EDI orders, blanket purchase agreements, individual purchase orders, or task orders for ordering services under this contract. Blanket Purchase Agreements shall not extend beyond the end of the contract period; all services and delivery shall be made and the contract terms and conditions shall continue in effect until the completion of the order. Orders for tasks which extend beyond the fiscal year for which funds are available shall include FAR 52.232-19 (Deviation – May 2003) Availability of Funds for the Next Fiscal Year. The purchase order shall specify the availability of funds and the period for which funds are available.
 - b. All task orders are subject to the terms and conditions of the contract. In the event of conflict between a task order and the contract, the contract will take precedence.
4. Performance of Services
 - a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity.
 - b. The Contractor agrees to render services only during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.
 - c. The ordering activity should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.

-
- d. Any Contractor travel required in the performance of IT Services must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel. Contractors cannot use GSA city pair contracts.
5. Stop-Work Order (FAR 52.242-15) (AUG 1989)
- a. The Contracting Officer may, at any time, by written order to the Contractor, require the Contractor to stop all, or any part, of the work called for by this contract for a period of 90 days after the order is delivered to the Contractor, and for any further period to which the parties may agree. The order shall be specifically identified as a stop-work order issued under this clause. Upon receipt of the order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the order during the period of work stoppage. Within a period of 90 days after a stop-work is delivered to the Contractor, or within any extension of that period to which the parties shall have agreed, the Contracting Officer shall either:
 - 1) Cancel the stop-work order; or
 - 2) Terminate the work covered by the order as provided in the Default, or the Termination for Convenience of the Government, clause of this contract.
 - b. If a stop-work order issued under this clause is canceled or the period of the order or any extension thereof expires, the Contractor shall resume work. The Contracting Officer shall make an equitable adjustment in the delivery schedule or contract price, or both, and the contract shall be modified, in writing, accordingly, if:
 - 1) The stop-work order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this contract; and
 - 2) The Contractor asserts its right to the adjustment within 30 days after the end of the period of work stoppage; provided, that, if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon the claim submitted at any time before final payment under this contract.
 - c. If a stop-work order is not canceled and the work covered by the order is terminated for the convenience of the Government, the Contracting Officer shall allow reasonable costs resulting from the stop-work order in arriving at the termination settlement.
 - d. If a stop-work order is not canceled and the work covered by the order is terminated for default, the Contracting Officer shall allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop-work order.
6. Inspection of Services
- The Inspection of Services–Fixed Price (AUG 1996) (Deviation – May 2003) clause at FAR 52.246-4 applies to firm-fixed price orders placed under this contract. The
-

Inspection–Time-and-Materials and Labor-Hour (JAN 1986) (Deviation – May 2003) clause at FAR 52.246-6 applies to time-and-materials and labor-hour orders placed under this contract.

7. Responsibilities of the Contractor

The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character. If the end product of a task order is software, then FAR 52.227-14 (Deviation – May 2003) Rights in Data – General, may apply.

8. Responsibilities of the Ordering Activity

Subject to security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite IT Services.

9. Independent Contractor

All IT Services performed by the Contractor under the terms of this contract shall be as an independent Contractor, and not as an agent or employee of the ordering activity.

10. Organizational Conflicts of Interest

a. Definitions.

“Contractor” means the person, firm, unincorporated association, joint venture, partnership, or corporation that is a party to this contract.

“Contractor and its affiliates” and “Contractor or its affiliates” refers to the Contractor, its chief executives, directors, officers, subsidiaries, affiliates, subcontractors at any tier, and consultants and any joint venture involving the Contractor, any entity into or with which the Contractor subsequently merges or affiliates, or any other successor or assignee of the Contractor.

An “Organizational conflict of interest” exists when the nature of the work to be performed under a proposed ordering activity contract, without some restriction on ordering activities by the Contractor and its affiliates, may either (i) result in an unfair competitive advantage to the Contractor or its affiliates or (ii) impair the Contractor’s or its affiliates’ objectivity in performing contract work.

b. To avoid an organizational or financial conflict of interest and to avoid prejudicing the best interests of the ordering activity, ordering activities may place restrictions on the Contractors, its affiliates, chief executives, directors, subsidiaries, and subcontractors at any tier when placing orders against schedule contracts. Such restrictions shall be consistent with FAR 9.505 and shall be designed to avoid, neutralize, or mitigate organizational conflicts of interest that might otherwise exist in situations related to individual orders placed against the schedule contract. Examples of situations, which may require restrictions, are provided at FAR 9.508.

11. Invoices

The Contractor, upon completion of the work ordered, shall submit invoices for IT services. Progress payments may be authorized by the ordering activity on individual orders if appropriate. Progress payments shall be based upon completion of defined milestones or interim products. Invoices shall be submitted monthly for recurring services performed during the preceding month.

12. Payments

For firm-fixed price orders the ordering activity shall pay the Contractor, upon submission of proper invoices or vouchers, the prices stipulated in this contract for service rendered and accepted. Progress payments shall be made only when authorized by the order. For time-and-materials orders, the Payments under Time-and-Materials and Labor-Hour Contracts at FAR 52.232-7 (DEC 2002), (Alternate II – Feb 2002) (Deviation – May 2003) applies to time-and-materials orders placed under this contract. For labor-hour orders, the Payment under Time-and-Materials and Labor-Hour Contracts at FAR 52.232-7 (DEC 2002), (Alternate II – Feb 2002) (Deviation – May 2003) applies to labor-hour orders placed under this contract. 52.216-31(Feb 2007) Time-and-Materials/Labor-Hour Proposal Requirements—Commercial Item Acquisition As prescribed in 16.601(e)(3), insert the following provision:

- a. The Government contemplates award of a Time-and-Materials or Labor-Hour type of contract resulting from this solicitation.
- b. The offeror must specify fixed hourly rates in its offer that include wages, overhead, general and administrative expenses, and profit. The offeror must specify whether the fixed hourly rate for each labor category applies to labor performed by:
 - 1) The offeror;
 - 2) Subcontractors; and/or
 - 3) Divisions, subsidiaries, or affiliates of the offeror under a common control.

13. Resumes

Resumes shall be provided to the GSA Contracting Officer or the user ordering activity upon request.

14. Incidental Support Costs

Incidental support costs are available outside the scope of this contract. The costs will be negotiated separately with the ordering activity in accordance with the guidelines set forth in the FAR.

15. Approval of Subcontracts

The ordering activity may require that the Contractor receive, from the ordering activity's Contracting Officer, written consent before placing any subcontract for furnishing any of the work called for in a task order.

16. Description of IT Services and Pricing
Refer to GSA Pricing Section.

Terms and Conditions Applicable to Highly Adaptive Cybersecurity Services (HACS) (Category: 54151HACS)

HACS includes a wide range of fields such as the seven-step Risk Management Framework services; information assurance; virus detection; network management; situational awareness and incident response; secure web hosting; and backup, security services and Security Operations Center (SOC) services. HACS vendors are cataloged under the 5 subcategories of High Value Asset Assessments, Risk and Vulnerability Assessments, Cyber Hunt, Incident Response, and Penetration Testing.

There are five subcategories under the HACS SIN:

- **High Value Asset Assessments** – Includes **Risk and Vulnerability Assessment (RVA)** which assesses threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations. See the section below on RVA for details on those services. **Security Architecture Review (SAR)** evaluates a subset of the agency’s HVA security posture to determine whether the agency has properly architected its cybersecurity solutions and ensures that agency leadership fully understands the risks inherent in the implemented cybersecurity solution. The SAR process utilizes in-person interviews, documentation reviews, and leading practice evaluations of the HVA environment and supporting systems. SAR provides a holistic analysis of how an HVA’s individual security components integrate and operate, including how data is protected during operations.
- **Systems Security Engineering (SSE)** – Identifies security vulnerabilities and minimizes or contains risks associated with these vulnerabilities spanning the Systems Development Life Cycle. SSE focuses on, but is not limited to, the following security areas: perimeter security, network security, endpoint security, application security, physical security, and data security.
- **Risk and Vulnerability Assessment** – Assesses threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations. The services offered in the RVA sub-category include Network Mapping, Vulnerability Scanning, Phishing Assessment, Wireless Assessment, Web Application Assessment, Operating System Security Assessment (OSSA), Database Assessment, and Penetration Testing.
- **Cyber Hunt** – Activities respond to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Cyber Hunts start with the premise that threat actors known to target some organizations in a specific industry or with specific systems are likely to also target other organizations in the same industry or with the same systems.

-
- **Incident Response** – Services help organizations impacted by a cybersecurity compromise determine the extent of the incident, remove the adversary from their systems, and restore their networks to a more secure state.
 - **Penetration Testing** – Is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network.

Order Level Materials (Special Item Number OLM)

OLMs are supplies and/or services acquired in direct support of an individual task or delivery order placed against a Schedule contract or BPA. OLM pricing is not established at the Schedule contract or BPA level, but at the order level. Since OLMs are identified and acquired at the order level, the ordering contracting officer (OCO) is responsible for making a fair and reasonable price determination for all OLMs.

OLMs are procured under a special ordering procedure that simplifies the process for acquiring supplies and services necessary to support individual task or delivery orders placed against a Schedule contract or BPA. Using this new procedure, ancillary supplies and services not known at the time of the Schedule award may be included and priced at the order level.

OLM SIN-Level Requirements/Ordering Instructions:

OLMs are:

- Purchased under the authority of the FSS Program
- Unknown until an order is placed
- Defined and priced at the ordering activity level in accordance with GSAR clause 552.238-115 Special Ordering Procedures for the Acquisition of Order-Level Materials. (Price analysis for OLMs is not conducted when awarding the FSS contract or FSS BPA; therefore, GSAR 538.270 and 538.271 do not apply to OLMs)
- Only authorized for use in direct support of another awarded SIN
- Only authorized for inclusion at the order level under a Time-and-Materials (T&M) or Labor-Hour (LH) Contract Line Item Number (CLIN)
- Subject to a Not To Exceed (NTE) ceiling price

OLMs are not:

- "Open Market Items"
- Items awarded under ancillary supplies/services or other direct cost (ODC) SINs (these items are defined, priced, and awarded at the FSS contract level)

OLM Pricing:

- Prices for items provided under the Order-Level Materials SIN must be inclusive of the Industrial Funding Fee (IFF).
- The value of OLMs in a task or delivery order, or the cumulative value of OLMs in orders against an FSS BPA awarded under an FSS contract, cannot exceed 33.33%.

Labor Category	Labor Category Description	Experience	Education
Computer Security Analyst, Junior	Fully applies basic principles, theories, and concepts to the development, maintenance, and implementation of information security standards, procedures, and guidelines. Solves moderately complex technical problems, ensuring that systems and organizational databases are protected from unauthorized access and use. Monitors systems, identifies threats, and handles disaster recovery operations.	3	Bachelors
Computer Security Analyst	Applies advanced principles, theories, and concepts to the development, maintenance, and implementation of information security standards, procedures, and guidelines. Solves complex technical problems, ensuring that systems and organizational databases are protected from unauthorized access and use. Monitors systems, identifies threats, and handles disaster recover operations. Interfaces with user community to understand their security needs, implementing procedures to accommodate them. Familiar with domain structures, network protocols, user authentication, digital signatures, firewalls, and security best practices.	5	Bachelors
Computer Security Analyst, Senior	Applies leading-edge principles, theories, and concepts to the development, maintenance, and implementation of information security standards, procedures, and guidelines. Solves very complex technical problems, ensuring that systems and organizational databases are protected from unauthorized access and use. Monitors systems, identifies threats, and handles disaster recovery operations. Interfaces with user community to understand their security needs, implementing procedures to accommodate them. Understands domain structures, network protocols, user authentication, digital signatures, firewalls, and security best practices. Identifies network vulnerabilities and recommends remedial action.	7	Bachelors
Program Manager	Provides team leadership and creativity in the development and implementation of services engagements. Directs multiple and complex projects or sub-projects, including project financials. Manages and leads large work teams. Sets objectives and priorities for the project staff. Assigns and reviews tasks, performance, and staffing requirements. Identifies and pursues new business opportunities within the existing client bases.	8	Bachelors
Project Manager	Manages projects of moderate risk and complexity. May have deputy responsibility for a large program/project. Oversees program/project budget and schedules. May have primary responsibility for program/project growth. Serves as primary customer contact. Total value of programs/projects is generally between \$10 million and \$25 million (life of contracts). May be responsible for programs/projects of a lesser dollar	7	Bachelors

Labor Category	Labor Category Description	Experience	Education
	value if they are more complex or developmental in nature.		
QA Analyst	Performs complex tasks related to specialized inspection and testing of project output to ensure that quality standards are met. Develops and refines processes related to quality control and project failure identification and design standards verification. Reviews project development documentation to ensure specifications are designed to meet inspection and testing standards. Initiates corrective action for procedural, product, or process deficiencies. Interfaces with customers, vendors, and various company departments to resolve quality problems and provide information. Participates in and may lead audits.	6	Bachelors
Software Engineer, Junior	Designs, develops, troubleshoots, and analyzes software programs. Performs systems modeling, simulation, and analysis. Designs and develops compilers, assemblers, utility programs, and operating systems. Advises hardware design engineers on machine characteristics that affect software systems, such as storage capacity, processing speed, and input/output requirements. As required, provides inputs for documentation of new or existing programs.	3	Bachelors
Software Engineer, Senior	Develops and applies advanced methods, theories, and research techniques in the investigation and solution of highly complex and difficult software applications and problems requiring the expert application of advanced knowledge. Plans, conducts, technically directs, and evaluates projects or major phases of significant projects, managing the efforts of engineers and technical support staff in the performance of assigned projects. Recommends corrections in technical applications and analysis. Provides technical consultation to other organizations.	10	Bachelors
Subject Matter Expert	High level of knowledge of client needs for special projects. May possess certifications in a specific technical or management discipline. Develops specifications for moderately complex applications and business information systems.	5	Bachelors
Subject Matter Expert, Senior	An expert in the subject matter field. Provides high level systems analysis, design, integration, documentation, and implementation advice on complex studies. Participates in a phases of study development. Possesses certifications in a specific technical or management discipline. Prepares and delivers senior management presentations and briefings as required.	8	Bachelors
Systems Analyst	Performs analysis, design, and development of simple to intermediate computer systems. Assists in the determination of user needs with the maintenance of single product modules and subsystems. Assists in the design and development of simple utility programs and operating systems.	5	Bachelors
Systems Engineer,	Analyzes existing systems and defines, designs, and develops new	3	Bachelors

Labor Category	Labor Category Description	Experience	Education
Junior	system requirements. Determines system specifications, input/output processes, and working parameters for hardware/software compatibility. Coordinates design of subsystems and integration of total system. Identifies, analyzes, and resolves program support deficiencies.		
Systems Engineer	Develops and applies advanced methods, theories, and research techniques in the investigation and solution of complex and difficult system design requirements and problems. Plans, conducts, and technically directs projects or major phases of significant projects. Reviews completion and implementation of systems additions and/or enhancements and recommends corrections in technical application and analysis to management. Evaluates vendor capabilities to provide required products or services.	6	Bachelors
Systems Engineer, Senior	Develops and applies advanced methods, theories, and research techniques in the investigation and solution of complex and difficult system design requirements and problems requiring the expert application of advanced knowledge. Plans, conducts, and technically directs projects or major phases of significant projects, managing the efforts of engineers and technical support staff in the performance of assigned projects. Reviews completion and implementation of systems additions and/or enhancements, and recommends corrections in technical application and analysis to management.	10	Bachelors
Support Specialist	Provides second-tier support to end users for either PC, server, or mainframe applications and hardware. Interacts with network services, software systems engineering, and/or applications development to restore service and/or identify and correct core problem. Simulates or recreates user problems to resolve operating difficulties. Recommends systems modifications to reduce user problems.	6	Bachelors
Support Specialist, Senior	Provides second-tier support to end users for either PC, server, or mainframe applications and hardware. Interacts with network services, software systems engineering, and/or applications development to restore service and/or identify and correct core problem. Simulates or recreates user problems to resolve operating difficulties. Recommends systems modifications to reduce user problems. Ensures the timely process through which problems are controlled. Includes problem recognition, research, isolation, resolution, and follow-up steps.	10	Bachelors
Database Administrator, Junior	Develops, implements, administers, and maintains policies and procedures for ensuring the security and integrity of database management systems. Implements data models, database designs, data access, and table maintenance codes. Resolves database	3	Bachelors

Labor Category	Labor Category Description	Experience	Education
	performance and capacity issues and replication and other distributed data issues.		
Database Administrator	Provides expertise and guidance in the use of database management systems. Designs, implements, and maintains databases with respect to access methods and time, device allocation, validation checks, file organization, indexing methods, protection and security, documentation, guidelines, and statistical methods. Establishes procedures for operations of the database and database management systems. Collects data elements and prepares database specifications. Develops, maintains, and controls the data dictionary.	6	Bachelors
Database Administrator, Senior	Provides expertise and guidance in the use of database management systems. Designs, implements, and maintains databases with respect to access methods and time, device allocation, validation checks, file organization, indexing methods, protection and security, documentation, guidelines, and statistical methods. Establishes procedures for operations of the database and database management systems. Collects data elements and prepares database specifications. Develops, maintains, and controls the data dictionary.	8	Bachelors
Program Manager - Cyber Security - (Junior)	Provides team leadership and creativity in the development and implementation of services engagements. Directs multiple and complex projects or sub-projects, including project financials. Manages and leads large work teams. Sets objectives and priorities for the project staff. Assigns and reviews tasks, performance, and staffing requirements. Identifies and pursues new business opportunities within the existing client base	2	Bachelors
Program Manager - Cyber Security - (Intermediate)	Provides team leadership and creativity in the development and implementation of services engagements. Directs multiple and complex projects or sub-projects, including project financials. Manages and leads large work teams. Sets objectives and priorities for the project staff. Assigns and reviews tasks, performance, and staffing requirements. Identifies and pursues new business opportunities within the existing client base	5	Bachelors
Program Manager - Cyber Security - (Senior)	Provides team leadership and creativity in the development and implementation of services engagements. Directs multiple and complex projects or sub-projects, including project financials. Manages and leads large work teams. Sets objectives and priorities for the project staff. Assigns and reviews tasks, performance, and staffing requirements. Identifies and pursues new business opportunities within the existing client base	8	Bachelors
Cybersecurity Project/Task Manager	Manages projects of moderate risk and complexity. May have deputy responsibility for a large program/project. Oversees	2	Bachelors

Labor Category	Labor Category Description	Experience	Education
(Junior)	program/project budget and schedules. May have primary responsibility for program/project growth. Serves as primary customer contact. Total value of programs/projects is generally between \$10 million and \$25 million (life of contracts). May be responsible for programs/projects of a lesser dollar value if they are more complex or developmental in nature.		
Cybersecurity Project/Task Manager (Intermediate)	Manages projects of moderate risk and complexity. May have deputy responsibility for a large program/project. Oversees program/project budget and schedules. May have primary responsibility for program/project growth. Serves as primary customer contact. Total value of programs/projects is generally between \$10 million and \$25 million (life of contracts). May be responsible for programs/projects of a lesser dollar value if they are more complex or developmental in nature.	5	Bachelors
Cybersecurity Project/Task Manager (Senior)	Manages projects of moderate risk and complexity. May have deputy responsibility for a large program/project. Oversees program/project budget and schedules. May have primary responsibility for program/project growth. Serves as primary customer contact. Total value of programs/projects is generally between \$10 million and \$25 million (life of contracts). May be responsible for programs/projects of a lesser dollar value if they are more complex or developmental in nature.	7	Bachelors
Information Security Specialist (Junior)	Under direct supervision, assists in developing and maintaining knowledgebase on changing regulatory, threat, and technology landscapes to continually develop or maintain security policies and standards, and ensure compliance throughout the organization.	2	Bachelors
Information Security Specialist (Intermediate)	Under general supervision, uses current information security technology disciplines and practices to ensure the confidentiality, integrity and availability of corporate information assets in accordance with established standards and procedures. Develops and maintains knowledgebase on changing regulatory, threat, and technology landscapes to continually develop or maintain security policies and standards, and ensure compliance throughout the organization.	5	Bachelors
Information Security Specialist (Senior)	Responsible for using current information security technology disciplines and practices to ensure the confidentiality, integrity and availability of corporate information assets in accordance with established standards and procedures. Develops and maintains knowledgebase on changing regulatory, threat, and technology landscapes to continually develop or maintain security policies and standards, and ensure compliance throughout the organization.	8	Bachelors
Subject Matter Expert - Cyber Security - (Junior)	High level of knowledge of client needs for special projects. May possess certifications in a specific technical or management	3	Bachelors

Labor Category	Labor Category Description	Experience	Education
	discipline. Develops specifications for moderately complex applications and business information systems.		
Subject Matter Expert - Cyber Security - (Intermediate)	An expert in the subject matter field. Provides high level systems analysis, design, integration, documentation, and implementation advice on complex studies. Possesses certifications in a specific technical or management discipline. Prepares and delivers senior management presentations and briefings as required.	5	Bachelors
Subject Matter Expert - Cyber Security - (Senior)	An expert in the subject matter field. Provides high level systems analysis, design, integration, documentation, and implementation advice on complex studies. Participates in a phases of study development. Possesses certifications in a specific technical or management discipline. Prepares and delivers senior management presentations and briefings as required.	8	Bachelors
Cybersecurity Network Engineer (Junior)	<p>Designs and plans network communications systems. Provides specifications and detailed schematics for network architecture. Conducts cost/benefit analysis and provides specific detailed information for hardware and software selection, implementation techniques and tools for the most efficient solution to meet business needs, including present and future capacity requirements. Conducts testing of network design. Responsible for monitoring network hardware operations to ensure properly set configuration options. Plans implementation of enhancements and upgrades to the network. Advises network users of hardware requirements, configurations, and limitations. Maintains technical expertise in all areas of network and computer hardware and software interconnection and interfacing, such as routers, multiplexers, firewalls, hubs, bridges, gateways, etc. Evaluates and reports on new communications technologies to enhance capabilities of the network. May be assigned responsibility for the management of the systems administration function, including associated staff.</p> <p>Works on assignments requiring considerable judgment and initiative. Develops solutions to routine technical problems of limited scope following detailed instructions. Work is supervised. Bachelor's (or equivalent) with 0 - 2 yrs of experience.</p>	2	Bachelors
Cybersecurity Network Engineer (Intermediate)	Designs and plans network communications systems. Provides specifications and detailed schematics for network architecture. Conducts cost/benefit analysis and provides specific detailed information for hardware and software selection, implementation techniques and tools for the most efficient solution to meet business needs, including present and future capacity requirements. Conducts testing of network design. Responsible for	5	Bachelors

Labor Category	Labor Category Description	Experience	Education
	<p>monitoring network hardware operations to ensure properly set configuration options. Plans implementation of enhancements and upgrades to the network. Advises network users of hardware requirements, configurations, and limitations. Maintains technical expertise in all areas of network and computer hardware and software interconnection and interfacing, such as routers, multiplexers, firewalls, hubs, bridges, gateways, etc. Evaluates and reports on new communications technologies to enhance capabilities of the network. May be assigned responsibility for the management of the systems administration function, including associated staff.</p> <p>Career level with a complete understanding and wide application of technical principles, theories and concepts. Working under only general direction, provides technical solutions to a wide range of difficult problems. Independently determines and develops approach to solutions. Bachelor's (or equivalent) with 5 - 7 yrs of experience, or a Master's and 3 to 5 yrs of experience.</p>		
Cybersecurity Network Engineer (Senior)	<p>Designs and plans network communications systems. Provides specifications and detailed schematics for network architecture. Conducts cost/benefit analysis and provides specific detailed information for hardware and software selection, implementation techniques and tools for the most efficient solution to meet business needs, including present and future capacity requirements. Conducts testing of network design. Responsible for monitoring network hardware operations to ensure properly set configuration options. Plans implementation of enhancements and upgrades to the network. Advises network users of hardware requirements, configurations, and limitations. Maintains technical expertise in all areas of network and computer hardware and software interconnection and interfacing, such as routers, multiplexers, firewalls, hubs, bridges, gateways, etc. Evaluates and reports on new communications technologies to enhance capabilities of the network. May be assigned responsibility for the management of the systems administration function, including associated staff.</p> <p>Considered an emerging authority, who applies extensive technical expertise. Develops technical solutions to complex problems. Exercises considerable latitude in determining objectives and approaches to assignment. Bachelor's (or equivalent) with 8 - 10 yrs of experience, or a Master's with 6 - 8 yrs of experience.</p>	8	Bachelors
Cybersecurity Technical	Writes, rewrites and/or edits technical documents such as technical	1	Bachelors

Labor Category	Labor Category Description	Experience	Education
Writer (Junior)	<p>procedure manuals, user manuals, programming manuals, service manuals, operational specifications, and related technical publications to communicate clearly and effectively technical specifications and instructions to a wide range of audiences. Acquires subject knowledge by interviewing product developers, observing performance of production methods, referring to technical specifications, blueprints, engineering illustrations, and trade journals. Oversees preparation of illustrative materials, selecting drawings, sketches, diagrams and charts. Conducts quality review of materials. Translates complex data into user-friendly text for print and electronic publications, such as technical journals, user and training manuals, government proposals, websites and podcasts. Gathers information through research, statistical reports and interviews with technical staff. Develops cataloging systems, and maintains records, files, electronic media and archiving of information for publications. Assists in preparing material for technical seminars and business forums. May be called upon to assist in technical or business presentations in such meetings as business or customer needs require. Selects or recommends use of layouts, graphics, drawings, tables, exhibits, illustrations, charts, or storyboards to amplify or clarify publications objectives.</p> <p>Works on assignments requiring considerable judgment and initiative. Develops solutions to routine technical problems of limited scope following detailed instructions. Work is supervised. Bachelor's (or equivalent) with 0 - 2 years of experience.</p>		
Cybersecurity Technical Writer (Intermediate)	<p>Writes, rewrites and/or edits technical documents such as technical procedure manuals, user manuals, programming manuals, service manuals, operational specifications, and related technical publications to communicate clearly and effectively technical specifications and instructions to a wide range of audiences. Acquires subject knowledge by interviewing product developers, observing performance of production methods, referring to technical specifications, blueprints, engineering illustrations, and trade journals. Oversees preparation of illustrative materials, selecting drawings, sketches, diagrams and charts. Conducts quality review of materials. Translates complex data into user-friendly text for print and electronic publications, such as technical journals, user and training manuals, government proposals, websites and podcasts. Gathers information through research, statistical reports and interviews with technical staff. Develops cataloging systems, and maintains records, files, electronic media and archiving of information for publications. Assists in preparing material for</p>	2	Bachelors

Labor Category	Labor Category Description	Experience	Education
	<p>technical seminars and business forums. May be called upon to assist in technical or business presentations in such meetings as business or customer needs require. Selects or recommends use of layouts, graphics, drawings, tables, exhibits, illustrations, charts, or storyboards to amplify or clarify publications objectives.</p> <p>Experienced with frequent use and application of technical standards, principles and theories. Works under general supervision, providing solutions to technical problems of moderate scope/complexity. Bachelor's (or equivalent) with 2 - 4years of experience, or a Master's with 0-2 years of experience.</p>		
Cybersecurity Technical Writer (Senior)	<p>Writes, rewrites and/or edits technical documents such as technical procedure manuals, user manuals, programming manuals, service manuals, operational specifications, and related technical publications to communicate clearly and effectively technical specifications and instructions to a wide range of audiences. Acquires subject knowledge by interviewing product developers, observing performance of production methods, referring to technical specifications, blueprints, engineering illustrations, and trade journals. Oversees preparation of illustrative materials, selecting drawings, sketches, diagrams and charts. Conducts quality review of materials. Translates complex data into user-friendly text for print and electronic publications, such as technical journals, user and training manuals, government proposals, websites and podcasts. Gathers information through research, statistical reports and interviews with technical staff. Develops cataloging systems, and maintains records, files, electronic media and archiving of information for publications. Assists in preparing material for technical seminars and business forums. May be called upon to assist in technical or business presentations in such meetings as business or customer needs require. Selects or recommends use of layouts, graphics, drawings, tables, exhibits, illustrations, charts, or storyboards to amplify or clarify publications objectives.</p> <p>Career level with a complete understanding and wide application of technical principles, theories and concepts. Working under only general direction, provides technical solutions to a wide range of difficult problems. Independently determines and develops approach to solutions. Bachelor's (or equivalent) with 5 - 7 years of experience, or a Master's and 3 to 5 years of experience.</p>	5	Bachelors
Systems Engineer - Cyber Security - (Junior)	Using a holistic approach, designs, develops, evaluates and modifies end-to-end systems and systems-oriented products through their entire life cycle. Generates quantifiable requirements based on	5	Bachelors

Labor Category	Labor Category Description	Experience	Education
	<p>customer description, system planning and design, and acquisition logistics. Ensures requirements comply with client requirements and government standards through formal verification methods. Translates high level product development strategies into system requirement specifications and works with other engineering disciplines to develop lower level detailed implementation requirements. Establishes and coordinates development of standards, practices, and procedures as related to the overall product development. Designs interfaces and brings system elements together so they work as a whole. Assesses performance using evaluation criteria and technical performance measures. Customer liaison and support for business development activities and to understand and shape requirements. Participates in system conceptual design and documentation of the design concepts. Translates high level product development strategies into system requirement specifications and works with multi-discipline engineering teams to develop lower level detailed requirements. Participates in design reviews of components (hardware and software) to ensure applicability to the current system and traceability of requirements through compliance verification and validation. Generates system level requirements verification procedures and customer acceptance test procedures. Reviews test plans/procedures and ensures they meet the objectives of the contractual requirements and participates in the testing process to validate requirements.</p> <p>Career level with a complete understanding and wide application of technical principles, theories and concepts. Working under only general direction, provides technical solutions to a wide range of difficult problems. Independently determines and develops approach to solutions. Bachelor's (or equivalent) with 5 - 7 yrs of experience, or a Master's and 3 to 5 yrs of experience.</p>		
Systems Engineer - Cyber Security - (Intermediate)	Using a holistic approach, designs, develops, evaluates and modifies end-to-end systems and systems-oriented products through their entire life cycle. Generates quantifiable requirements based on customer description, system planning and design, and acquisition logistics. Ensures requirements comply with client requirements and government standards through formal verification methods. Translates high level product development strategies into system requirement specifications and works with other engineering disciplines to develop lower level detailed implementation requirements. Establishes and coordinates development of standards, practices, and procedures as related to the overall	7	Bachelors

Labor Category	Labor Category Description	Experience	Education
	<p>product development. Designs interfaces and brings system elements together so they work as a whole. Assesses performance using evaluation criteria and technical performance measures. Customer liaison and support for business development activities and to understand and shape requirements. Participates in system conceptual design and documentation of the design concepts. Translates high level product development strategies into system requirement specifications and works with multi-discipline engineering teams to develop lower level detailed requirements. Participates in design reviews of components (hardware and software) to ensure applicability to the current system and traceability of requirements through compliance verification and validation. Generates system level requirements verification procedures and customer acceptance test procedures. Reviews test plans/procedures and ensures they meet the objectives of the contractual requirements and participates in the testing process to validate requirements.</p> <p>Career level with a complete understanding and wide application of technical principles, theories and concepts. Working under only general direction, provides technical solutions to a wide range of difficult problems. Independently determines and develops approach to solutions. Bachelor's (or equivalent) with 5 - 7 yrs of experience, or a Master's and 3 to 5 yrs of experience.</p>		
Systems Engineer - Cyber Security - (Senior)	<p>Using a holistic approach, designs, develops, evaluates and modifies end-to-end systems and systems-oriented products through their entire life cycle. Generates quantifiable requirements based on customer description, system planning and design, and acquisition logistics. Ensures requirements comply with client requirements and government standards through formal verification methods. Translates high level product development strategies into system requirement specifications and works with other engineering disciplines to develop lower level detailed implementation requirements. Establishes and coordinates development of standards, practices, and procedures as related to the overall product development. Designs interfaces and brings system elements together so they work as a whole. Assesses performance using evaluation criteria and technical performance measures. Customer liaison and support for business development activities and to understand and shape requirements. Participates in system conceptual design and documentation of the design concepts. Translates high level product development strategies into system requirement specifications and works with multi-discipline</p>	8	Bachelors

Labor Category	Labor Category Description	Experience	Education
	<p>engineering teams to develop lower level detailed requirements. Participates in design reviews of components (hardware and software) to ensure applicability to the current system and traceability of requirements through compliance verification and validation. Generates system level requirements verification procedures and customer acceptance test procedures. Reviews test plans/procedures and ensures they meet the objectives of the contractual requirements and participates in the testing process to validate requirements.</p> <p>Considered an emerging authority, who applies extensive technical expertise. Develops technical solutions to complex problems. Exercises considerable latitude in determining objectives and approaches to assignment. Bachelor's (or equivalent) with 8 - 10 yrs of experience, or a Master's with 6 - 8 yrs of experience.</p>		
Cybersecurity System Administrator (Junior)	<p>Maintains smooth operation of multi-user computer systems, including coordination with network engineers. Monitors and manages system resources, including CPU usage, disk usage, and response times to maintain operating efficiency. Performs systems security administration functions, including creating user profiles and accounts. Other duties may include setting up administrator accounts, maintaining system documentation, tuning system performance, installing system wide software and allocating mass storage space. Interacts with users and evaluates vendor products. Makes recommendations to purchase hardware and software, coordinates installation and provides backup recovery. Develops and monitors policies and standards for allocation related to the use of computing resources. May be assigned responsibility for less experienced staff.</p> <p>Experienced with frequent use and application of technical standards, principles and theories. Works under general supervision, providing solutions to technical problems of moderate scope/complexity. Bachelor's (or equivalent) with 2 - 4yrs of experience, or a Master's with 0-2 yrs of experience.</p>	2	Bachelors
Cybersecurity System Administrator (Intermediate)	<p>Maintains smooth operation of multi-user computer systems, including coordination with network engineers. Monitors and manages system resources, including CPU usage, disk usage, and response times to maintain operating efficiency. Performs systems security administration functions, including creating user profiles and accounts. Other duties may include setting up administrator accounts, maintaining system documentation, tuning system performance, installing system wide software and allocating mass</p>	5	Bachelors

Labor Category	Labor Category Description	Experience	Education
	<p>storage space. Interacts with users and evaluates vendor products. Makes recommendations to purchase hardware and software, coordinates installation and provides backup recovery. Develops and monitors policies and standards for allocation related to the use of computing resources. May be assigned responsibility for less experienced staff.</p> <p>Career level with a complete understanding and wide application of technical principles, theories and concepts. Working under only general direction, provides technical solutions to a wide range of difficult problems. Independently determines and develops approach to solutions. Bachelor's (or equivalent) with 5 - 7 yrs of experience, or a Master's and 3 to 5 yrs of experience.</p>		
Cybersecurity System Administrator (Senior)	<p>Maintains smooth operation of multi-user computer systems, including coordination with network engineers. Monitors and manages system resources, including CPU usage, disk usage, and response times to maintain operating efficiency. Performs systems security administration functions, including creating user profiles and accounts. Other duties may include setting up administrator accounts, maintaining system documentation, tuning system performance, installing system wide software and allocating mass storage space. Interacts with users and evaluates vendor products. Makes recommendations to purchase hardware and software, coordinates installation and provides backup recovery. Develops and monitors policies and standards for allocation related to the use of computing resources. May be assigned responsibility for less experienced staff.</p> <p>Considered an emerging authority, who applies extensive technical expertise. Develops technical solutions to complex problems. Exercises considerable latitude in determining objectives and approaches to assignment. Bachelor's (or equivalent) with 8 - 10 yrs of experience, or a Master's with 6 - 8 yrs of experience.</p>	8	Bachelors
Cybersecurity Architect (Junior)	<p>Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes. Ensures that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines. Defines and documents how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment.</p>	2	Bachelors

Labor Category	Labor Category Description	Experience	Education
	<p>Analyzes candidate architectures, allocates security services, and selects security mechanisms. Evaluates security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents. Determines the protection needs (i.e., security controls) for the information system(s) and network(s) and documents appropriately. Translates proposed capabilities into technical requirements. Performs security reviews, identify gaps in security architecture, and develop a security risk management plan. Provides input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials). Document sand addresses organization's information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition life cycle. Writes detailed functional specifications that document the security architecture development process.</p> <p>Experienced with frequent use and application of technical standards, principles and theories. Works under general supervision, providing solutions to technical problems of moderate scope/complexity. Bachelor's (or equivalent) with 2 - 4yrs of experience, or a Master's with 0-2 yrs of experience.</p>		
Cybersecurity Architect (Intermediate)	<p>Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes. Ensures that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines. Defines and documents how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment. Analyzes candidate architectures, allocates security services, and selects security mechanisms. Evaluates security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents. Determines the protection needs (i.e., security controls) for the information system(s) and network(s) and documents appropriately. Translates proposed capabilities into technical requirements. Performs security reviews, identify gaps in security architecture, and develop a security risk</p>	5	Bachelors

Labor Category	Labor Category Description	Experience	Education
	<p>management plan. Provides input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials). Document sand addresses organization's information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition life cycle. Writes detailed functional specifications that document the security architecture development process.</p> <p>Career level with a complete understanding and wide application of technical principles, theories and concepts. Working under only general direction, provides technical solutions to a wide range of difficult problems. Independently determines and develops approach to solutions. Bachelor's (or equivalent) with 5 - 7 yrs of experience, or a Master's and 3 to 5 yrs of experience.</p>		
Cybersecurity Architect (Senior)	<p>Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes. Ensures that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines. Defines and documents how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment. Analyzes candidate architectures, allocates security services, and selects security mechanisms. Evaluates security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents. Determines the protection needs (i.e., security controls) for the information system(s) and network(s) and documents appropriately. Translates proposed capabilities into technical requirements. Performs security reviews, identify gaps in security architecture, and develop a security risk management plan. Provides input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials). Document sand addresses organization's information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition life cycle. Writes detailed functional specifications that document the security architecture development</p>	10	Bachelors

Labor Category	Labor Category Description	Experience	Education
	<p>process.</p> <p>Considered a recognized authority within the company. Works on unusually complex technical problems and provides solutions which are highly innovative. Determines and pursues courses of action necessary to obtain desired results. Bachelor's (or equivalent) with 10 - 12 yrs of experience or a Master's with 8 - 10 yrs of experience.</p>		
<p>Cybersecurity Engineer (Junior)</p>	<p>Monitor, analyze, and detect Cyber events and incidents within information systems and networks under general supervision. Assist with integrated, dynamic Cyberdefense, coordinate and maintain security toolsets to support organizations' continuous monitoring and ongoing authorization programs, establish a framework by which cyber risk can be measured and quantified in the marketplace. Determines security requirements by evaluating business strategies and requirements; researching information security standards; conducting system security and vulnerability analyses and risk assessments; studying architecture/platform; identifying integration issues; preparing cost estimates. Implements security systems by specifying intrusion detection methodologies and equipment; directing equipment and software installation and calibration; preparing preventive and reactive measures; creating, transmitting, and maintaining keys; providing technical support; completing documentation. Verifies security systems by developing and implementing test scripts. Maintains security by monitoring and ensuring compliance to standards, policies, and procedures; conducting incident response analyses; developing and conducting training programs. Responsible for the design, development, implementation, and integration of a DoD IA architectures, systems, or system components for use within computing, network, and enclave environments. Ensure that the architecture and design of development and operational systems are functional and secure. This include designs for program of record systems and special purpose processing nodes with platform IT interconnectivity.</p> <p>Experienced with frequent use and application of technical standards, principles and theories. Works under general supervision, providing solutions to technical problems of moderate scope/complexity. Bachelor's (or equivalent) with 2 - 4yrs of experience, or a Master's with 0-2 yrs of experience.</p>	<p>2</p>	<p>Bachelors</p>
<p>Cybersecurity Engineer (Intermediate)</p>	<p>Monitor, analyze, and detect Cyber events and incidents within information systems and networks under general supervision. Assist with integrated, dynamic Cyberdefense, coordinate and maintain security toolsets to support organizations' continuous monitoring</p>	<p>8</p>	<p>Bachelors</p>

Labor Category	Labor Category Description	Experience	Education
	<p>and ongoing authorization programs, establish a framework by which cyber risk can be measured and quantified in the marketplace. Determines security requirements by evaluating business strategies and requirements; researching information security standards; conducting system security and vulnerability analyses and risk assessments; studying architecture/platform; identifying integration issues; preparing cost estimates. Implements security systems by specifying intrusion detection methodologies and equipment; directing equipment and software installation and calibration; preparing preventive and reactive measures; creating, transmitting, and maintaining keys; providing technical support; completing documentation. Verifies security systems by developing and implementing test scripts. Maintains security by monitoring and ensuring compliance to standards, policies, and procedures; conducting incident response analyses; developing and conducting training programs. Responsible for the design, development, implementation, and integration of a DoD IA architectures, systems, or system components for use within computing, network, and enclave environments. Ensure that the architecture and design of development and operational systems are functional and secure. This include designs for program of record systems and special purpose processing nodes with platform IT interconnectivity.</p> <p>Considered an emerging authority, who applies extensive technical expertise. Develops technical solutions to complex problems. Exercises considerable latitude in determining objectives and approaches to assignment. Bachelor's (or equivalent) with 8 - 10 yrs of experience, or a Master's with 6 - 8 yrs of experience.</p>		
Cybersecurity Engineer (Senior)	<p>Monitor, analyze, and detect Cyber events and incidents within information systems and networks under general supervision. Assist with integrated, dynamic Cyberdefense, coordinate and maintain security toolsets to support organizations' continuous monitoring and ongoing authorization programs, establish a framework by which cyber risk can be measured and quantified in the marketplace. Determines security requirements by evaluating business strategies and requirements; researching information security standards; conducting system security and vulnerability analyses and risk assessments; studying architecture/platform; identifying integration issues; preparing cost estimates. Implements security systems by specifying intrusion detection methodologies and equipment; directing equipment and software installation and calibration; preparing preventive and reactive measures; creating, transmitting, and maintaining keys; providing technical support;</p>	10	Bachelors

Labor Category	Labor Category Description	Experience	Education
	<p>completing documentation. Verifies security systems by developing and implementing test scripts. Maintains security by monitoring and ensuring compliance to standards, policies, and procedures; conducting incident response analyses; developing and conducting training programs. Responsible for the design, development, implementation, and integration of a DoD IA architectures, systems, or system components for use within computing, network, and enclave environments. Ensure that the architecture and design of development and operational systems are functional and secure. This include designs for program of record systems and special purpose processing nodes with platform IT interconnectivity.</p> <p>Considered a recognized authority within the company. Works on unusually complex technical problems and provides solutions which are highly innovative. Determines and pursues courses of action necessary to obtain desired results. Bachelor's (or equivalent) with 10 - 12 yrs of experience or a Master's with 8 - 10 yrs of experience.</p>		
Cyber Threat Analyst (Junior)	<p>Working as expert, conduct research and evaluate technical and all-source intelligence with specific emphasis on network operations and cyber warfare tactics, techniques, and procedures focused on the threat to networked weapons platforms and US and DoD information networks. Analyzes network events to determine the impact on current operations and conduct all-source research to determine advisory capability and intent. Prepares assessments and cyber threat profiles of current events based on the sophisticated collection, research and analysis of classified and open source information. Correlates threat data from various sources. Develops and maintains analytical procedures to meet changing requirements and ensure maximum operations. Collects data using a combination of standard intelligence methods and business processes. Produces high-quality papers, presentations, recommendations, and findings for senior US government intelligence and network operations officials.</p> <p>Experienced with frequent use and application of technical standards, principles and theories. Works under general supervision, providing solutions to technical problems of moderate scope/complexity. Bachelor's (or equivalent) with 2 - 4yrs of experience, or a Master's with 0-2 yrs of experience.</p>	2	Bachelors
Cyber Threat Analyst (Intermediate)	Working as expert, conduct research and evaluate technical and all-source intelligence with specific emphasis on network operations and cyber warfare tactics, techniques, and procedures focused on the threat to networked weapons platforms and US and DoD	5	Bachelors

Labor Category	Labor Category Description	Experience	Education
	<p>information networks. Analyzes network events to determine the impact on current operations and conduct all-source research to determine advisory capability and intent. Prepares assessments and cyber threat profiles of current events based on the sophisticated collection, research and analysis of classified and open source information. Correlates threat data from various sources. Develops and maintains analytical procedures to meet changing requirements and ensure maximum operations. Collects data using a combination of standard intelligence methods and business processes. Produces high-quality papers, presentations, recommendations, and findings for senior US government intelligence and network operations officials.</p> <p>Career level with a complete understanding and wide application of technical principles, theories and concepts. Working under only general direction, provides technical solutions to a wide range of difficult problems. Independently determines and develops approach to solutions. Bachelor's (or equivalent) with 5 - 7 yrs of experience, or a Master's and 3 to 5 yrs of experience.</p>		
<p>Cyber Threat Analyst (Senior)</p>	<p>Working as expert, conduct research and evaluate technical and all-source intelligence with specific emphasis on network operations and cyber warfare tactics, techniques, and procedures focused on the threat to networked weapons platforms and US and DoD information networks. Analyzes network events to determine the impact on current operations and conduct all-source research to determine advisory capability and intent. Prepares assessments and cyber threat profiles of current events based on the sophisticated collection, research and analysis of classified and open source information. Correlates threat data from various sources. Develops and maintains analytical procedures to meet changing requirements and ensure maximum operations. Collects data using a combination of standard intelligence methods and business processes. Produces high-quality papers, presentations, recommendations, and findings for senior US government intelligence and network operations officials.</p> <p>Considered an emerging authority, who applies extensive technical expertise. Develops technical solutions to complex problems. Exercises considerable latitude in determining objectives and approaches to assignment. Bachelor's (or equivalent) with 8 - 10 yrs of experience, or a Master's with 6 - 8 yrs of experience.</p>	<p>8</p>	<p>Bachelors</p>
<p>Cybersecurity DevOps Engineer (Junior)</p>	<p>Provides expertise and direction in the development and/or modification of computer-based scientific, technical, and business</p>	<p>2</p>	<p>Bachelors</p>

Labor Category	Labor Category Description	Experience	Education
	<p>software systems. Uses expertise to design develop, code, test, and debug software. May work in one or several areas, such as equipment or software design, engineering evaluation or test, configuration management procedures, statistical analysis and modeling. Works with users to define existing or new system scope and objectives. Provides analytical support and technical advice during the conceptualization, development, and implementation phases. Plans and schedules new applications systems projects with user, systems software, and computer center operations personnel, including the identification of objectives, time frames, costs, and manpower requirements. Performs tasks necessary to ensure the identification and documentation of hazards within software systems using various analysis tools and techniques. Reviews and evaluates systems and software for adherence to government or commercial directives, standards, guidelines, and criteria concerning software safety and systems safety. Confirms design mitigations are captured in the design and its documentation and verifies implementation. May perform as a project lead with the responsibility for the instruction, assigning, direction, and monitoring of the performance of assigned systems developers / analyst working on a specific project.</p> <p>Experienced with frequent use and application of technical standards, principles and theories. Works under general supervision, providing solutions to technical problems of moderate scope/complexity. Bachelor's (or equivalent) with 2 - 4yrs of experience, or a Master's with 0-2 yrs of experience.</p>		
Cybersecurity DevOps Engineer (Intermediate)	<p>Provides expertise and direction in the development and/or modification of computer-based scientific, technical, and business software systems. Uses expertise to design develop, code, test, and debug software. May work in one or several areas, such as equipment or software design, engineering evaluation or test, configuration management procedures, statistical analysis and modeling. Works with users to define existing or new system scope and objectives. Provides analytical support and technical advice during the conceptualization, development, and implementation phases. Plans and schedules new applications systems projects with user, systems software, and computer center operations personnel, including the identification of objectives, time frames, costs, and manpower requirements. Performs tasks necessary to ensure the identification and documentation of hazards within software systems using various analysis tools and techniques. Reviews and evaluates systems and software for adherence to</p>	5	Bachelors

Labor Category	Labor Category Description	Experience	Education
	<p>government or commercial directives, standards, guidelines, and criteria concerning software safety and systems safety. Confirms design mitigations are captured in the design and its documentation and verifies implementation. May perform as a project lead with the responsibility for the instruction, assigning, direction, and monitoring of the performance of assigned systems developers / analyst working on a specific project.</p> <p>Career level with a complete understanding and wide application of technical principles, theories and concepts. Working under only general direction, provides technical solutions to a wide range of difficult problems. Independently determines and develops approach to solutions. Bachelor's (or equivalent) with 5 - 7 yrs of experience, or a Master's and 3 to 5 yrs of experience.</p>		
Cybersecurity DevOps Engineer (Senior)	<p>Provides expertise and direction in the development and/or modification of computer-based scientific, technical, and business software systems. Uses expertise to design develop, code, test, and debug software. May work in one or several areas, such as equipment or software design, engineering evaluation or test, configuration management procedures, statistical analysis and modeling. Works with users to define existing or new system scope and objectives. Provides analytical support and technical advice during the conceptualization, development, and implementation phases. Plans and schedules new applications systems projects with user, systems software, and computer center operations personnel, including the identification of objectives, time frames, costs, and manpower requirements. Performs tasks necessary to ensure the identification and documentation of hazards within software systems using various analysis tools and techniques. Reviews and evaluates systems and software for adherence to government or commercial directives, standards, guidelines, and criteria concerning software safety and systems safety. Confirms design mitigations are captured in the design and its documentation and verifies implementation. May perform as a project lead with the responsibility for the instruction, assigning, direction, and monitoring of the performance of assigned systems developers / analyst working on a specific project.</p> <p>Considered an emerging authority, who applies extensive technical expertise. Develops technical solutions to complex problems. Exercises considerable latitude in determining objectives and approaches to assignment. Bachelor's (or equivalent) with 8 - 10 yrs of experience, or a Master's with 6 - 8 yrs of experience.</p>	8	Bachelors

Labor Category	Labor Category Description	Experience	Education
Database Administrator - Cyber Security - (Junior)	Develops, implements, administers, and maintains policies and procedures for ensuring that security and integrity of database management systems. Implements data models, database designs, data access, and table maintenance codes. Resolves database performance and capacity issues and replication and other distributed data issues.	3	Bachelors
Database Administrator - Cyber Security - (Intermediate)	Provides expertise and guidance in the use of database management systems. Designs, implements, and maintains databases with respect to access methods and time, device allocation, validation checks, file organization, indexing methods, protection and security, documentation, guidelines, and statistical methods. Establishes procedures for operations of the database and database management systems. Collects data elements and prepares database specifications. Develops, maintains, and controls the data dictionary.	6	Bachelors
Database Administrator - Cyber Security - (Senior)	Provides expertise and guidance in the use of database management systems. Designs, implements, and maintains databases with respect to access methods and time, device allocation, validation checks, file organization, indexing methods, protection and security, documentation, guidelines, and statistical methods. Establishes procedures for operations of the database and database management systems. Collects data elements and prepares database specifications. Develops, maintains, and controls the data dictionary.	8	Bachelors
Cybersecurity Database Engineer (Junior)	<p>Designs, develops, builds, analyzes, evaluates and installs database management systems to include database modeling and design, relational database architecture, metadata and repository creation and configuration management. Uses data mapping, data mining and data transformational analysis tools to design and develop databases. Determines data storage and optimum storage requirements. Prepares system requirements, source analysis and process analyses and design throughout the database implementation. Evaluates, sizes and selects technology components, such as software, hardware, and networking capabilities, for database management systems and application databases. Writes and tunes SQL queries for performance and scalability. Implements comprehensive backup and database replication solutions.</p> <p>Experienced with frequent use and application of technical standards, principles and theories. Works under general supervision, providing solutions to technical problems of moderate scope/complexity. Bachelor's (or equivalent) with 2 - 4yrs of</p>	2	Bachelors

Labor Category	Labor Category Description	Experience	Education
Cybersecurity Database Engineer (Intermediate)	<p>experience, or a Master's with 0-2 yrs of experience.</p> <p>Designs, develops, builds, analyzes, evaluates and installs database management systems to include database modeling and design, relational database architecture, metadata and repository creation and configuration management. Uses data mapping, data mining and data transformational analysis tools to design and develop databases. Determines data storage and optimum storage requirements. Prepares system requirements, source analysis and process analyses and design throughout the database implementation. Evaluates, sizes and selects technology components, such as software, hardware, and networking capabilities, for database management systems and application databases. Writes and tunes SQL queries for performance and scalability. Implements comprehensive backup and database replication solutions.</p> <p>Career level with a complete understanding and wide application of technical principles, theories and concepts. Working under only general direction, provides technical solutions to a wide range of difficult problems. Independently determines and develops approach to solutions. Bachelor's (or equivalent) with 5 - 7 yrs of experience, or a Master's and 3 to 5 yrs of experience.</p>	5	Bachelors
Cybersecurity Database Engineer (Senior)	<p>Designs, develops, builds, analyzes, evaluates and installs database management systems to include database modeling and design, relational database architecture, metadata and repository creation and configuration management. Uses data mapping, data mining and data transformational analysis tools to design and develop databases. Determines data storage and optimum storage requirements. Prepares system requirements, source analysis and process analyses and design throughout the database implementation. Evaluates, sizes and selects technology components, such as software, hardware, and networking capabilities, for database management systems and application databases. Writes and tunes SQL queries for performance and scalability. Implements comprehensive backup and database replication solutions.</p> <p>Considered an emerging authority, who applies extensive technical expertise. Develops technical solutions to complex problems. Exercises considerable latitude in determining objectives and approaches to assignment. Bachelor's (or equivalent) with 8 - 10 yrs of experience, or a Master's with 6 - 8 yrs of experience.</p>	8	Bachelors
User Experience / User	Develops custom programs for web sites that will attract and	2	Bachelors

Labor Category	Labor Category Description	Experience	Education
Interface Engineer (Junior)	<p>appeal to users, and provide desired information. Creates web applications and components from the requirements stage, through design, through production deployment. Possesses a thorough knowledge of programming and server software operations. Develops new Web applications through packaged and customized applications. Creates Web front-end user interface to new or existing databases using a combination of HTML, SQL, C, VB or other languages to make business applications accessible. Designs and implements user-driven templates, databases and interfaces for ease of use. May create company-wide Intranet. Develops database-driven Web interfaces for rapid, real-time information sharing. Develops external Web portals allowing users to input and retrieve accurate information. Experienced in graphics, layout, scripting, programming, as well as development involving compatibility and seamless integration with various technologies such as Java and ColdFusion.</p> <p>Experienced with frequent use and application of technical standards, principles and theories. Works under general supervision, providing solutions to technical problems of moderate scope/complexity. Bachelor's (or equivalent) with 2 - 4yrs of experience, or a Master's with 0-2 yrs of experience.</p>		
User Experience / User Interface Engineer (Intermediate)	<p>Develops custom programs for web sites that will attract and appeal to users, and provide desired information. Creates web applications and components from the requirements stage, through design, through production deployment. Possesses a thorough knowledge of programming and server software operations. Develops new Web applications through packaged and customized applications. Creates Web front-end user interface to new or existing databases using a combination of HTML, SQL, C, VB or other languages to make business applications accessible. Designs and implements user-driven templates, databases and interfaces for ease of use. May create company-wide Intranet. Develops database-driven Web interfaces for rapid, real-time information sharing. Develops external Web portals allowing users to input and retrieve accurate information. Experienced in graphics, layout, scripting, programming, as well as development involving compatibility and seamless integration with various technologies such as Java and ColdFusion.</p> <p>Career level with a complete understanding and wide application of technical principles, theories and concepts. Working under only general direction, provides technical solutions to a wide range of</p>	5	Bachelors

Labor Category	Labor Category Description	Experience	Education
	<p>difficult problems. Independently determines and develops approach to solutions. Bachelor's (or equivalent) with 5 - 7 yrs of experience, or a Master's and 3 to 5 yrs of experience.</p>		
<p>User Experience / User Interface Engineer (Senior)</p>	<p>Develops custom programs for web sites that will attract and appeal to users, and provide desired information. Creates web applications and components from the requirements stage, through design, through production deployment. Possesses a thorough knowledge of programming and server software operations. Develops new Web applications through packaged and customized applications. Creates Web front-end user interface to new or existing databases using a combination of HTML, SQL, C, VB or other languages to make business applications accessible. Designs and implements user-driven templates, databases and interfaces for ease of use. May create company-wide Intranet. Develops database-driven Web interfaces for rapid, real-time information sharing. Develops external Web portals allowing users to input and retrieve accurate information. Experienced in graphics, layout, scripting, programming, as well as development involving compatibility and seamless integration with various technologies such as Java and ColdFusion.</p> <p>Considered an emerging authority, who applies extensive technical expertise. Develops technical solutions to complex problems. Exercises considerable latitude in determining objectives and approaches to assignment. Bachelor's (or equivalent) with 8 - 10 yrs of experience, or a Master's with 6 - 8 yrs of experience.</p>	<p>8</p>	<p>Bachelors</p>
<p>Application Security SME / Lead (Junior)</p>	<p>Collaborates with various project managers, application development, security, and operations teams, to improve the security of applications across the SDLC. Has a thorough knowledge of Agile SDLC methodologies and DevSecOps practices. Has strong secure application development, testing and automation experience. Performs and reviews the results of code security tests, validates the results of the vulnerability findings, and provides guidance on remediation efforts. Develops and maintains integration between application security products, bug trackers and CI/CD tools. Understands application security to include mitigating threats (i.e Denial of Service, Brute Force, Buffer Overflows, Input Validation, e.t.c) . Supports technical team with code review in relation to application service pack releases. Participates in requirements reviews, environments compliance support to ensure security best practices are included in the builds. Participates in architecture reviews, change control board reviews, and assist with validation of CCB approved changes. Performs application</p>	<p>2</p>	<p>Bachelors</p>

Labor Category	Labor Category Description	Experience	Education
	<p>vulnerability assessments, security control validations, documents and tracks findings to closure. Analyzes application vulnerability findings and POA&Ms to provide recommendations and assist with implementation of changes. Performs analysis for application and web specific vulnerability scan results (Nessus, Appdetective, webinspect, Appscan). Coordinates with Technical Team Leads and Security Administrators for remediation plans. Provides guidance on and oversees secure application coding practices conducted by other technical teams. Supports technical teams with code review in relation to application service pack releases.</p> <p>Experienced with frequent use and application of technical standards, principles and theories. Works under general supervision, providing solutions to technical problems of moderate scope/complexity. Bachelor's (or equivalent) with 2 - 4yrs of experience, or a Master's with 0-2 yrs of experience.</p>		
<p>Application Security SME / Lead (Intermediate)</p>	<p>Collaborates with various project managers, application development, security, and operations teams, to improve the security of applications across the SDLC. Has a thorough knowledge of Agile SDLC methodologies and DevSecOps practices. Has strong secure application development, testing and automation experience. Performs and reviews the results of code security tests, validates the results of the vulnerability findings, and provides guidance on remediation efforts. Develops and maintains integration between application security products, bug trackers and CI/CD tools. Understands application security to include mitigating threats (i.e Denial of Service, Brute Force, Buffer Overflows, Input Validation, e.t.c) . Supports technical team with code review in relation to application service pack releases. Participates in requirements reviews, environments compliance support to ensure security best practices are included in the builds. Participates in architecture reviews, change control board reviews, and assist with validation of CCB approved changes. Performs application vulnerability assessments, security control validations, documents and tracks findings to closure. Analyzes application vulnerability findings and POA&Ms to provide recommendations and assist with implementation of changes. Performs analysis for application and web specific vulnerability scan results (Nessus, Appdetective, webinspect, Appscan). Coordinates with Technical Team Leads and Security Administrators for remediation plans. Provides guidance on and oversees secure application coding practices conducted by other technical teams. Supports technical teams with code review in relation to application service pack releases.</p>	<p>5</p>	<p>Bachelors</p>

Labor Category	Labor Category Description	Experience	Education
	<p>Career level with a complete understanding and wide application of technical principles, theories and concepts. Working under only general direction, provides technical solutions to a wide range of difficult problems. Independently determines and develops approach to solutions. Bachelor's (or equivalent) with 5 - 7 yrs of experience, or a Master's and 3 to 5 yrs of experience.</p>		
<p>Application Security SME / Lead (Senior)</p>	<p>Collaborates with various project managers, application development, security, and operations teams, to improve the security of applications across the SDLC. Has a thorough knowledge of Agile SDLC methodologies and DevSecOps practices. Has strong secure application development, testing and automation experience. Performs and reviews the results of code security tests, validates the results of the vulnerability findings, and provides guidance on remediation efforts. Develops and maintains integration between application security products, bug trackers and CI/CD tools. Understands application security to include mitigating threats (i.e Denial of Service, Brute Force, Buffer Overflows, Input Validation, e.t.c) . Supports technical team with code review in relation to application service pack releases. Participates in requirements reviews, environments compliance support to ensure security best practices are included in the builds. Participates in architecture reviews, change control board reviews, and assist with validation of CCB approved changes. Performs application vulnerability assessments, security control validations, documents and tracks findings to closure. Analyzes application vulnerability findings and POA&Ms to provide recommendations and assist with implementation of changes. Performs analysis for application and web specific vulnerability scan results (Nessus, Appdetective, webinspect, Appscan). Coordinates with Technical Team Leads and Security Administrators for remediation plans. Provides guidance on and oversees secure application coding practices conducted by other technical teams. Supports technical teams with code review in relation to application service pack releases.</p> <p>Considered an emerging authority, who applies extensive technical expertise. Develops technical solutions to complex problems. Exercises considerable latitude in determining objectives and approaches to assignment. Bachelor's (or equivalent) with 8 - 10 yrs of experience, or a Master's with 6 - 8 yrs of experience.</p>	<p>8</p>	<p>Bachelors</p>
<p>Cybersecurity Software Developer (Junior)</p>	<p>Provides expertise and direction in the development and/or modification of computer-based scientific, technical, and business software systems. Uses expertise to design develop, code, test, and</p>	<p>2</p>	<p>Bachelors</p>

Labor Category	Labor Category Description	Experience	Education
	<p>debug software. May work in one or several areas, such as equipment or software design, engineering evaluation or test, configuration management procedures, statistical analysis and modeling. Works with users to define existing or new system scope and objectives. Provides analytical support and technical advice during the conceptualization, development, and implementation phases. Plans and schedules new applications systems projects with user, systems software, and computer center operations personnel, including the identification of objectives, time frames, costs, and manpower requirements. Performs tasks necessary to ensure the identification and documentation of hazards within software systems using various analysis tools and techniques. Reviews and evaluates systems and software for adherence to government or commercial directives, standards, guidelines, and criteria concerning software safety and systems safety. Confirms design mitigations are captured in the design and its documentation and verifies implementation. May perform as a project lead with the responsibility for the instruction, assigning, direction, and monitoring of the performance of assigned systems developers / analyst working on a specific project.</p> <p>Experienced with frequent use and application of technical standards, principles and theories. Works under general supervision, providing solutions to technical problems of moderate scope/complexity. Bachelor's (or equivalent) with 2 - 4yrs of experience, or a Master's with 0-2 yrs of experience.</p>		
Cybersecurity Software Developer (Intermediate)	Provides expertise and direction in the development and/or modification of computer-based scientific, technical, and business software systems. Uses expertise to design develop, code, test, and debug software. May work in one or several areas, such as equipment or software design, engineering evaluation or test, configuration management procedures, statistical analysis and modeling. Works with users to define existing or new system scope and objectives. Provides analytical support and technical advice during the conceptualization, development, and implementation phases. Plans and schedules new applications systems projects with user, systems software, and computer center operations personnel, including the identification of objectives, time frames, costs, and manpower requirements. Performs tasks necessary to ensure the identification and documentation of hazards within software systems using various analysis tools and techniques. Reviews and evaluates systems and software for adherence to government or commercial directives, standards, guidelines, and	5	Bachelors

Labor Category	Labor Category Description	Experience	Education
	<p>criteria concerning software safety and systems safety. Confirms design mitigations are captured in the design and its documentation and verifies implementation. May perform as a project lead with the responsibility for the instruction, assigning, direction, and monitoring of the performance of assigned systems developers / analyst working on a specific project.</p> <p>Career level with a complete understanding and wide application of technical principles, theories and concepts. Working under only general direction, provides technical solutions to a wide range of difficult problems. Independently determines and develops approach to solutions. Bachelor's (or equivalent) with 5 - 7 yrs of experience, or a Master's and 3 to 5 yrs of experience.</p>		
Cybersecurity Software Developer (Senior)	<p>Provides expertise and direction in the development and/or modification of computer-based scientific, technical, and business software systems. Uses expertise to design develop, code, test, and debug software. May work in one or several areas, such as equipment or software design, engineering evaluation or test, configuration management procedures, statistical analysis and modeling. Works with users to define existing or new system scope and objectives. Provides analytical support and technical advice during the conceptualization, development, and implementation phases. Plans and schedules new applications systems projects with user, systems software, and computer center operations personnel, including the identification of objectives, time frames, costs, and manpower requirements. Performs tasks necessary to ensure the identification and documentation of hazards within software systems using various analysis tools and techniques. Reviews and evaluates systems and software for adherence to government or commercial directives, standards, guidelines, and criteria concerning software safety and systems safety. Confirms design mitigations are captured in the design and its documentation and verifies implementation. May perform as a project lead with the responsibility for the instruction, assigning, direction, and monitoring of the performance of assigned systems developers / analyst working on a specific project.</p> <p>Considered an emerging authority, who applies extensive technical expertise. Develops technical solutions to complex problems. Exercises considerable latitude in determining objectives and approaches to assignment. Bachelor's (or equivalent) with 8 - 10 yrs of experience, or a Master's with 6 - 8 yrs of experience.</p>	8	Bachelors
Cybersecurity	Under general supervision, audits new and existing information	2	Bachelors

Labor Category	Labor Category Description	Experience	Education
Information Assurance Engineer (Junior)	systems applications to ensure that appropriate controls exist, that processing is efficient and accurate, and that systems procedures are in compliance with corporate standards		
Cybersecurity Information Assurance Engineer (Intermediate)	Under general supervision, develops information systems assurance programs and control guidelines, assists in resolving technical problems, priorities, and methods.	5	Bachelors
Cybersecurity Information Assurance Engineer (Senior)	Responsible for all activities relating to information assurance procedures and systems. Develops information systems assurance programs and control guidelines. Confers with and advises subordinates on administrative policies and procedures and resolving technical problems, priorities, and methods. Consults with and advises other sections regarding internal controls and security procedures. Prepares activity and progress reports relating to the information systems audit function.	8	Bachelors
Cybersecurity Incident Responder (Junior)	<p>Contribute to the functional management and oversight of the collection and analysis of threat intelligence, event analysis, automation and orchestration, and incident response. Contribute to the execution of Cyber Security operations, incident response, and investigations spanning across all functions of the Corporate Security organization. Rapidly and accurately determine the source of a security incident and moving quickly to identify and apply containment, mitigation, and remediation steps. Leverage the corporate incident case management solution to document and report on incidents to meet audit, compliance and legal requirements. Conduct in-depth root cause analysis on complex malware and user/system behavior events. Gather and analyze forensic evidence for cyber security incidents and investigations. Design and implement threat and event analysis automation to improve the speed and accuracy of incident identification and mitigation. Develop and document enhanced event analysis and incident response processes and procedures. Serve as a member of an incident response and monitoring team. Perform investigations to identify attack vectors, confirm infections, and suggest mitigation tactics. Develops technical solutions and Standard Operating Procedures (SOPs) for incident response, network security, advanced analytic tools, and data visualization techniques. Collaborate with technical teams to identify, resolve, and mitigate vulnerabilities.</p> <p>Experienced with frequent use and application of technical standards, principles and theories. Works under general supervision, providing solutions to technical problems of moderate scope/complexity. Bachelor's (or equivalent) with 2 - 4yrs of</p>	2	Bachelors

Labor Category	Labor Category Description	Experience	Education
Cybersecurity Incident Responder (Intermediate)	<p>experience, or a Master's with 0-2 yrs of experience.</p> <p>Contribute to the functional management and oversight of the collection and analysis of threat intelligence, event analysis, automation and orchestration, and incident response. Contribute to the execution of Cyber Security operations, incident response, and investigations spanning across all functions of the Corporate Security organization. Rapidly and accurately determine the source of a security incident and moving quickly to identify and apply containment, mitigation, and remediation steps. Leverage the corporate incident case management solution to document and report on incidents to meet audit, compliance and legal requirements. Conduct in-depth root cause analysis on complex malware and user/system behavior events. Gather and analyze forensic evidence for cyber security incidents and investigations. Design and implement threat and event analysis automation to improve the speed and accuracy of incident identification and mitigation. Develop and document enhanced event analysis and incident response processes and procedures. Serve as a member of an incident response and monitoring team. Perform investigations to identify attack vectors, confirm infections, and suggest mitigation tactics. Develops technical solutions and Standard Operating Procedures (SOPs) for incident response, network security, advanced analytic tools, and data visualization techniques. Collaborate with technical teams to identify, resolve, and mitigate vulnerabilities.</p> <p>Career level with a complete understanding and wide application of technical principles, theories and concepts. Working under only general direction, provides technical solutions to a wide range of difficult problems. Independently determines and develops approach to solutions. Bachelor's (or equivalent) with 5 - 7 yrs of experience, or a Master's and 3 to 5 yrs of experience.</p>	5	Bachelors
Cybersecurity Incident Responder (Senior)	<p>Contribute to the functional management and oversight of the collection and analysis of threat intelligence, event analysis, automation and orchestration, and incident response. Contribute to the execution of Cyber Security operations, incident response, and investigations spanning across all functions of the Corporate Security organization. Rapidly and accurately determine the source of a security incident and moving quickly to identify and apply containment, mitigation, and remediation steps. Leverage the corporate incident case management solution to document and report on incidents to meet audit, compliance and legal requirements. Conduct in-depth root cause analysis on complex</p>	8	Bachelors

Labor Category	Labor Category Description	Experience	Education
	<p>malware and user/system behavior events. Gather and analyze forensic evidence for cyber security incidents and investigations. Design and implement threat and event analysis automation to improve the speed and accuracy of incident identification and mitigation. Develop and document enhanced event analysis and incident response processes and procedures. Serve as a member of an incident response and monitoring team. Perform investigations to identify attack vectors, confirm infections, and suggest mitigation tactics. Develops technical solutions and Standard Operating Procedures (SOPs) for incident response, network security, advanced analytic tools, and data visualization techniques. Collaborate with technical teams to identify, resolve, and mitigate vulnerabilities.</p> <p>Considered an emerging authority, who applies extensive technical expertise. Develops technical solutions to complex problems. Exercises considerable latitude in determining objectives and approaches to assignment. Bachelor's (or equivalent) with 8 - 10 yrs of experience, or a Master's with 6 - 8 yrs of experience.</p>		
Penetration Tester (Junior)	<p>Monitor, analyze, and detect Cyber events and incidents within information systems and networks under general supervision. Assist with integrated, dynamic Cyberdefense, coordinate and maintain security toolsets to support organizations' continuous monitoring and ongoing authorization programs, establish a framework by which cyber risk can be measured and quantified in the marketplace. Determines security requirements by evaluating business strategies and requirements; researching information security standards; conducting system security and vulnerability analyses and risk assessments; studying architecture/platform; identifying integration issues; preparing cost estimates. Implements security systems by specifying intrusion detection methodologies and equipment; directing equipment and software installation and calibration; preparing preventive and reactive measures; creating, transmitting, and maintaining keys; providing technical support; completing documentation. Verifies security systems by developing and implementing test scripts. Maintains security by monitoring and ensuring compliance to standards, policies, and procedures; conducting incident response analyses; developing and conducting training programs. Responsible for the design, development, implementation, and integration of a DoD IA architectures, systems, or system components for use within computing, network, and enclave environments. Ensure that the architecture and design of development and operational systems are functional and secure.</p>	2	Bachelors

Labor Category	Labor Category Description	Experience	Education
	<p>This include designs for program of record systems and special purpose processing nodes with platform IT interconnectivity.</p> <p>Experienced with frequent use and application of technical standards, principles and theories. Works under general supervision, providing solutions to technical problems of moderate scope/complexity. Bachelor's (or equivalent) with 2 - 4yrs of experience, or a Master's with 0-2 yrs of experience.</p>		
<p>Penetration Tester (Intermediate)</p>	<p>Monitor, analyze, and detect Cyber events and incidents within information systems and networks under general supervision. Assist with integrated, dynamic Cyberdefense, coordinate and maintain security toolsets to support organizations' continuous monitoring and ongoing authorization programs, establish a framework by which cyber risk can be measured and quantified in the marketplace. Determines security requirements by evaluating business strategies and requirements; researching information security standards; conducting system security and vulnerability analyses and risk assessments; studying architecture/platform; identifying integration issues; preparing cost estimates. Implements security systems by specifying intrusion detection methodologies and equipment; directing equipment and software installation and calibration; preparing preventive and reactive measures; creating, transmitting, and maintaining keys; providing technical support; completing documentation. Verifies security systems by developing and implementing test scripts. Maintains security by monitoring and ensuring compliance to standards, policies, and procedures; conducting incident response analyses; developing and conducting training programs. Responsible for the design, development, implementation, and integration of a DoD IA architectures, systems, or system components for use within computing, network, and enclave environments. Ensure that the architecture and design of development and operational systems are functional and secure. This include designs for program of record systems and special purpose processing nodes with platform IT interconnectivity.</p> <p>Career level with a complete understanding and wide application of technical principles, theories and concepts. Working under only general direction, provides technical solutions to a wide range of difficult problems. Independently determines and develops approach to solutions. Bachelor's (or equivalent) with 5 - 7 yrs of experience, or a Master's and 3 to 5 yrs of experience.</p>	<p>5</p>	<p>Bachelors</p>
<p>Penetration Tester (Senior)</p>	<p>Monitor, analyze, and detect Cyber events and incidents within information systems and networks under general supervision. Assist</p>	<p>10</p>	<p>Bachelors</p>

Labor Category	Labor Category Description	Experience	Education
	<p>with integrated, dynamic Cyberdefense, coordinate and maintain security toolsets to support organizations' continuous monitoring and ongoing authorization programs, establish a framework by which cyber risk can be measured and quantified in the marketplace. Determines security requirements by evaluating business strategies and requirements; researching information security standards; conducting system security and vulnerability analyses and risk assessments; studying architecture/platform; identifying integration issues; preparing cost estimates. Implements security systems by specifying intrusion detection methodologies and equipment; directing equipment and software installation and calibration; preparing preventive and reactive measures; creating, transmitting, and maintaining keys; providing technical support; completing documentation. Verifies security systems by developing and implementing test scripts. Maintains security by monitoring and ensuring compliance to standards, policies, and procedures; conducting incident response analyses; developing and conducting training programs. Responsible for the design, development, implementation, and integration of a DoD IA architectures, systems, or system components for use within computing, network, and enclave environments. Ensure that the architecture and design of development and operational systems are functional and secure. This include designs for program of record systems and special purpose processing nodes with platform IT interconnectivity.</p> <p>Considered a recognized authority within the company. Works on unusually complex technical problems and provides solutions which are highly innovative. Determines and pursues courses of action necessary to obtain desired results. Bachelor's (or equivalent) with 10 - 12 yrs of experience or a Master's with 8 - 10 yrs of experience.</p>		
Computer Forensics Analyst (Junior)	<p>Support customers in proactively planning for and defending against a variety of cyber threats using both commercial and custom technology and threat intelligence sources. Perform in-depth forensic analysis on captured logs, network traffic collections, volatile memory or host images to identify and trace breach indicators and develop actionable threat intelligence. Forensically secure, preserve, and capture volatile or physical disk data from workstations, laptops, servers, and network infrastructure devices thereby establishing that the evidential integrity of the data is not compromised. Respond, investigate, and prevent cyber-attacks and breaches. Perform incident response and forensics activities. Provide detailed briefings and reports post-incident as well as ongoing support. Recover data from computer hard drives and</p>	2	Bachelors

Labor Category	Labor Category Description	Experience	Education
	<p>other data storage devices, such as zip and flash drives, that have been deleted, damaged or otherwise manipulated. Protect computers from infiltration, determine how a computer was broken into or recover lost files. Trace the development and application of technical threat intelligence in the cyber-attack lifecycle. Manage the multi-source threat intelligence fusion and production of technical intelligence reports. Background in dynamic and static malware analysis and sandboxing with the ability to reverse engineer and debug malware samples using tools such as IDA Pro</p> <p>Experienced with frequent use and application of technical standards, principles and theories. Works under general supervision, providing solutions to technical problems of moderate scope/complexity. Bachelor's (or equivalent) with 2 - 4yrs of experience, or a Master's with 0-2 yrs of experience.</p>		
Computer Forensics Analyst (Intermediate)	<p>Support customers in proactively planning for and defending against a variety of cyber threats using both commercial and custom technology and threat intelligence sources. Perform in-depth forensic analysis on captured logs, network traffic collections, volatile memory or host images to identify and trace breach indicators and develop actionable threat intelligence. Forensically secure, preserve, and capture volatile or physical disk data from workstations, laptops, servers, and network infrastructure devices thereby establishing that the evidential integrity of the data is not compromised. Respond, investigate, and prevent cyber-attacks and breaches. Perform incident response and forensics activities. Provide detailed briefings and reports post-incident as well as ongoing support. Recover data from computer hard drives and other data storage devices, such as zip and flash drives, that have been deleted, damaged or otherwise manipulated. Protect computers from infiltration, determine how a computer was broken into or recover lost files. Trace the development and application of technical threat intelligence in the cyber-attack lifecycle. Manage the multi-source threat intelligence fusion and production of technical intelligence reports. Background in dynamic and static malware analysis and sandboxing with the ability to reverse engineer and debug malware samples using tools such as IDA Pro</p> <p>Career level with a complete understanding and wide application of technical principles, theories and concepts. Working under only general direction, provides technical solutions to a wide range of difficult problems. Independently determines and develops approach to solutions. Bachelor's (or equivalent) with 5 - 7 yrs of</p>	5	Bachelors

Labor Category	Labor Category Description	Experience	Education
Computer Forensics Analyst (Senior)	<p>experience, or a Master's and 3 to 5 yrs of experience.</p> <p>Support customers in proactively planning for and defending against a variety of cyber threats using both commercial and custom technology and threat intelligence sources. Perform in-depth forensic analysis on captured logs, network traffic collections, volatile memory or host images to identify and trace breach indicators and develop actionable threat intelligence. Forensically secure, preserve, and capture volatile or physical disk data from workstations, laptops, servers, and network infrastructure devices thereby establishing that the evidential integrity of the data is not compromised. Respond, investigate, and prevent cyber-attacks and breaches. Perform incident response and forensics activities. Provide detailed briefings and reports post-incident as well as ongoing support. Recover data from computer hard drives and other data storage devices, such as zip and flash drives, that have been deleted, damaged or otherwise manipulated. Protect computers from infiltration, determine how a computer was broken into or recover lost files. Trace the development and application of technical threat intelligence in the cyber-attack lifecycle. Manage the multi-source threat intelligence fusion and production of technical intelligence reports. Background in dynamic and static malware analysis and sandboxing with the ability to reverse engineer and debug malware samples using tools such as IDA Pro</p> <p>Considered an emerging authority, who applies extensive technical expertise. Develops technical solutions to complex problems. Exercises considerable latitude in determining objectives and approaches to assignment. Bachelor's (or equivalent) with 8 - 10 yrs of experience, or a Master's with 6 - 8 yrs of experience.</p>	8	Bachelors
CLOUD Software Engineer - Mid	<p>Develops and applies advanced methods, theories, and research techniques in the investigation and solution of highly complex and difficult software applications and problems requiring the expert application of advanced knowledge. Plans, conducts, technically directs, and evaluates projects or major phases of significant projects, managing the efforts of engineers and technical support staff in the performance of assigned projects. Recommends corrections in technical applications and analysis. Provides technical consultation to other organizations. Focused on providing support to the adoption of, migration to or governance/management of Cloud computing. Provides migration services that support activities associated with assessing Cloud solutions, refactoring workloads for Cloud solutions, migrating legacy or other systems to Cloud solutions, providing management/governance of Cloud solutions,</p>	5	Bachelors

Labor Category	Labor Category Description	Experience	Education
	DevOps, developing cloud native applications or other Cloud oriented activities.		
CLOUD Software Engineer - Sr	Develops and applies advanced methods, theories, and research techniques in the investigation and solution of highly complex and difficult software applications and problems requiring the expert application of advanced knowledge. Plans, conducts, technically directs, and evaluates projects or major phases of significant projects, managing the efforts of engineers and technical support staff in the performance of assigned projects. Recommends corrections in technical applications and analysis. Provides technical consultation to other organizations. Focused on providing support to the adoption of, migration to or governance/management of Cloud computing. Provides migration services that support activities associated with assessing Cloud solutions, refactoring workloads for Cloud solutions, migrating legacy or other systems to Cloud solutions, providing management/governance of Cloud solutions, DevOps, developing cloud native applications or other Cloud oriented activities.	8	Bachelors
CLOUD System Engineering Expert	Develops and applies advanced methods, theories, and research techniques in the investigation and solution of complex and difficult system design requirements and problems requiring the expert application of advanced knowledge. Plans, conducts, and technically directs projects or major phases of significant projects, managing the efforts of engineers and technical support staff in the performance of assigned projects. Reviews completion and implementation of systems additions and/or enhancements, and recommends corrections in technical application and analysis to management. Focused on providing support to the adoption of, migration to or governance/management of Cloud computing. Provides migration services that support activities associated with assessing Cloud solutions, refactoring workloads for Cloud solutions, migrating legacy or other systems to Cloud solutions, providing management/governance of Cloud solutions, DevOps, developing cloud native applications or other Cloud oriented activities.	8	Bachelors
CLOUD Software Engineer - Expert	Develops and applies advanced methods, theories, and research techniques in the investigation and solution of highly complex and difficult software applications and problems requiring the expert application of advanced knowledge. Plans, conducts, technically directs, and evaluates projects or major phases of significant projects, managing the efforts of engineers and technical support staff in the performance of assigned projects. Recommends corrections in technical applications and analysis. Provides technical	10	Bachelors

Labor Category	Labor Category Description	Experience	Education
	consultation to other organizations. Focused on providing support to the adoption of, migration to or governance/management of Cloud computing. Provides migration services that support activities associated with assessing Cloud solutions, refactoring workloads for Cloud solutions, migrating legacy or other systems to Cloud solutions, providing management/governance of Cloud solutions, DevOps, developing cloud native applications or other Cloud oriented activities.		
Administrative Assistant	Provide administrative support to project teams. Assist in the preparation of deliverables.	2	High School

Education/Experience Substitution Policy

We recognize that successful performance depends on having personnel with the right skills and experience. These skills and experience are acquired through a proper mix of education and professional experience. We have found that skills required to support advanced technology efforts, today's problems and tomorrow's challenges, are not always supported by the traditional combination of formal education and work experience. Therefore, we have incorporated substitution allowances between equivalent education and experience in order to provide the quality of services required by the customer at the most reasonable price.

The following tables present substitution equivalencies for education and experience requirements.

Substitutions for Educational Requirements

Additional years of related experience may be substituted for degree requirements.

Degree Requirement	Equivalent Experience Substitution
High School	GED
Associate's	High School plus two years related experience
Bachelor's	High school plus four years related experience or Associate degree plus two years related experience
Master's	Bachelor's degree plus two years related experience or Six years related experience
Doctorate / PhD	Master's degree plus two years or Eight years related experience

Substitutions for Work Experience Requirements.

A related degree may be substituted for years of related work experience.

Degree	Equivalent Years of Experience
Bachelor's	Two
Master's	Four
Doctorate/PhD	Six

Successful completion of higher education which has not yet resulted in a degree may be counted as one year of experience for each year of college completed.

GSA Labor Rates

GSA Price List Hourly Rates are inclusive of Industrial Funding Fee (IFF)

Labor Category	Contractor or Customer Facility or Both	10/16/2020 - 10/15/2021	10/16/2021 - 10/15/2022	10/16/2022 - 10/15/2023
Computer Security Analyst, Junior	Both	\$78.53	\$80.50	\$82.51
Computer Security Analyst	Both	\$124.69	\$127.81	\$131.00
Computer Security Analyst, Senior	Both	\$153.99	\$157.84	\$161.79
Program Manager	Both	\$176.18	\$180.58	\$185.10
Project Manager	Both	\$132.93	\$136.26	\$139.66
QA Analyst	Both	\$117.11	\$120.04	\$123.04
Software Engineer, Junior	Both	\$102.40	\$104.96	\$107.58
Software Engineer, Senior	Both	\$136.57	\$139.99	\$143.48
Subject Matter Expert	Both	\$140.51	\$144.02	\$147.62
Subject Matter Expert, Senior	Both	\$196.82	\$201.74	\$206.78
Systems Analyst	Both	\$98.03	\$100.48	\$102.99
Systems Engineer, Junior	Both	\$106.22	\$108.88	\$111.60
Systems Engineer	Both	\$128.52	\$131.74	\$135.03
Systems Engineer, Senior	Both	\$149.00	\$152.73	\$156.55
Support Specialist	Both	\$62.25	\$63.80	\$65.40
Support Specialist, Senior	Both	\$77.55	\$79.49	\$81.48
Database Administrator, Junior	Both	\$85.83	\$87.98	\$90.18
Database Administrator	Both	\$140.14	\$143.64	\$147.23
Database Administrator, Senior	Both	\$147.09	\$150.76	\$154.53
Program Manager - Cyber Security - (Junior)	Contractor Facility	-	\$193.61	\$198.45
Program Manager - Cyber Security - (Intermediate)	Contractor Facility	-	\$207.26	\$212.44
Program Manager - Cyber Security - (Senior)	Contractor Facility	-	\$252.11	\$258.41
Cybersecurity Project/Task Manager (Junior)	Contractor Facility	-	\$101.53	\$104.07
Cybersecurity Project/Task Manager (Intermediate)	Contractor Facility	-	\$115.33	\$118.21
Cybersecurity Project/Task Manager (Senior)	Contractor Facility	-	\$158.00	\$161.95

Labor Category	Contractor or Customer Facility or Both	10/16/2020 - 10/15/2021	10/16/2021 - 10/15/2022	10/16/2022 - 10/15/2023
Information Security Specialist (Junior)	Contractor Facility	-	\$94.38	\$96.74
Information Security Specialist (Intermediate)	Contractor Facility	-	\$119.61	\$122.60
Information Security Specialist (Senior)	Contractor Facility	-	\$147.81	\$151.51
Subject Matter Expert - Cyber Security - (Junior)	Contractor Facility	-	\$92.85	\$95.17
Subject Matter Expert - Cyber Security - (Intermediate)	Contractor Facility	-	\$158.93	\$162.90
Subject Matter Expert - Cyber Security - (Senior)	Contractor Facility	-	\$241.90	\$247.95
Cybersecurity Network Engineer (Junior)	Contractor Facility	-	\$96.06	\$98.46
Cybersecurity Network Engineer (Intermediate)	Contractor Facility	-	\$118.25	\$121.21
Cybersecurity Network Engineer (Senior)	Contractor Facility	-	\$158.74	\$162.71
Cybersecurity Technical Writer (Junior)	Contractor Facility	-	\$65.79	\$67.43
Cybersecurity Technical Writer (Intermediate)	Contractor Facility	-	\$79.37	\$81.35
Cybersecurity Technical Writer (Senior)	Contractor Facility	-	\$99.17	\$101.65
Systems Engineer - Cyber Security - (Junior)	Contractor Facility	-	\$123.64	\$126.73
Systems Engineer - Cyber Security - (Intermediate)	Contractor Facility	-	\$144.75	\$148.37
Systems Engineer - Cyber Security - (Senior)	Contractor Facility	-	\$178.09	\$182.54
Cybersecurity System Administrator (Junior)	Contractor Facility	-	\$93.56	\$95.90
Cybersecurity System Administrator (Intermediate)	Contractor Facility	-	\$115.64	\$118.53
Cybersecurity System Administrator (Senior)	Contractor Facility	-	\$137.93	\$141.38
Cybersecurity Architect (Junior)	Contractor Facility	-	\$104.63	\$107.25
Cybersecurity Architect (Intermediate)	Contractor Facility	-	\$126.31	\$129.47

Labor Category	Contractor or Customer Facility or Both	10/16/2020 - 10/15/2021	10/16/2021 - 10/15/2022	10/16/2022 - 10/15/2023
Cybersecurity Architect (Senior)	Contractor Facility	-	\$201.61	\$206.65
Cybersecurity Engineer (Junior)	Contractor Facility	-	\$104.63	\$107.25
Cybersecurity Engineer (Intermediate)	Contractor Facility	-	\$149.70	\$153.44
Cybersecurity Engineer (Senior)	Contractor Facility	-	\$168.97	\$173.19
Cyber Threat Analyst (Junior)	Contractor Facility	-	\$86.58	\$88.74
Cyber Threat Analyst (Intermediate)	Contractor Facility	-	\$94.53	\$96.89
Cyber Threat Analyst (Senior)	Contractor Facility	-	\$131.96	\$135.26
Cybersecurity DevOps Engineer (Junior)	Contractor Facility	-	\$100.61	\$103.13
Cybersecurity DevOps Engineer (Intermediate)	Contractor Facility	-	\$130.46	\$133.72
Cybersecurity DevOps Engineer (Senior)	Contractor Facility	-	\$166.31	\$170.47
Database Administrator - Cyber Security - (Junior)	Contractor Facility	-	\$102.93	\$105.50
Database Administrator - Cyber Security - (Intermediate)	Contractor Facility	-	\$161.38	\$165.41
Database Administrator - Cyber Security - (Senior)	Contractor Facility	-	\$168.39	\$172.60
Cybersecurity Database Engineer (Junior)	Contractor Facility	-	\$100.80	\$103.32
Cybersecurity Database Engineer (Intermediate)	Contractor Facility	-	\$128.91	\$132.13
Cybersecurity Database Engineer (Senior)	Contractor Facility	-	\$149.45	\$153.19
User Experience / User Interface Engineer (Junior)	Contractor Facility	-	\$94.39	\$96.75
User Experience / User Interface Engineer (Intermediate)	Contractor Facility	-	\$116.60	\$119.52
User Experience / User Interface Engineer (Senior)	Contractor Facility	-	\$137.71	\$141.15
Application Security SME / Lead (Junior)	Contractor Facility	-	\$104.63	\$107.25

Labor Category	Contractor or Customer Facility or Both	10/16/2020 - 10/15/2021	10/16/2021 - 10/15/2022	10/16/2022 - 10/15/2023
Application Security SME / Lead (Intermediate)	Contractor Facility	-	\$126.31	\$129.47
Application Security SME / Lead (Senior)	Contractor Facility	-	\$181.33	\$185.86
Cybersecurity Software Developer (Junior)	Contractor Facility	-	\$100.61	\$103.13
Cybersecurity Software Developer (Intermediate)	Contractor Facility	-	\$130.46	\$133.72
Cybersecurity Software Developer (Senior)	Contractor Facility	-	\$145.75	\$149.39
Cybersecurity Information Assurance Engineer (Junior)	Contractor Facility	-	\$94.38	\$96.74
Cybersecurity Information Assurance Engineer (Intermediate)	Contractor Facility	-	\$119.61	\$122.60
Cybersecurity Information Assurance Engineer (Senior)	Contractor Facility	-	\$147.81	\$151.51
Cybersecurity Incident Responder (Junior)	Contractor Facility	-	\$104.63	\$107.25
Cybersecurity Incident Responder (Intermediate)	Contractor Facility	-	\$126.31	\$129.47
Cybersecurity Incident Responder (Senior)	Contractor Facility	-	\$149.70	\$153.44
Penetration Tester (Junior)	Contractor Facility	-	\$102.08	\$104.63
Penetration Tester (Intermediate)	Contractor Facility	-	\$146.05	\$149.70
Penetration Tester (Senior)	Contractor Facility	-	\$164.85	\$168.97
Computer Forensics Analyst (Junior)	Contractor Facility	-	\$114.56	\$117.42
Computer Forensics Analyst (Intermediate)	Contractor Facility	-	\$130.32	\$133.58
Computer Forensics Analyst (Senior)	Contractor Facility	-	\$149.70	\$153.44
Program Manager - Cyber Security - (Junior)	Customer Facility	-	\$180.57	\$185.08
Program Manager - Cyber Security - (Intermediate)	Customer Facility	-	\$193.30	\$198.13
Program Manager - Cyber Security - (Senior)	Customer Facility	-	\$235.13	\$241.01

Labor Category	Contractor or Customer Facility or Both	10/16/2020 - 10/15/2021	10/16/2021 - 10/15/2022	10/16/2022 - 10/15/2023
Cybersecurity Project/Task Manager (Junior)	Customer Facility	-	\$94.70	\$97.07
Cybersecurity Project/Task Manager (Intermediate)	Customer Facility	-	\$107.57	\$110.26
Cybersecurity Project/Task Manager (Senior)	Customer Facility	-	\$147.36	\$151.04
Information Security Specialist (Junior)	Customer Facility	-	\$88.02	\$90.22
Information Security Specialist (Intermediate)	Customer Facility	-	\$111.56	\$114.35
Information Security Specialist (Senior)	Customer Facility	-	\$137.86	\$141.31
Subject Matter Expert - Cyber Security - (Junior)	Customer Facility	-	\$86.60	\$88.77
Subject Matter Expert - Cyber Security - (Intermediate)	Customer Facility	-	\$148.23	\$151.94
Subject Matter Expert - Cyber Security - (Senior)	Customer Facility	-	\$225.62	\$231.26
Cybersecurity Network Engineer (Junior)	Customer Facility	-	\$89.59	\$91.83
Cybersecurity Network Engineer (Intermediate)	Customer Facility	-	\$110.28	\$113.04
Cybersecurity Network Engineer (Senior)	Customer Facility	-	\$148.05	\$151.75
Cybersecurity Technical Writer (Junior)	Customer Facility	-	\$61.36	\$62.89
Cybersecurity Technical Writer (Intermediate)	Customer Facility	-	\$74.03	\$75.88
Cybersecurity Technical Writer (Senior)	Customer Facility	-	\$92.49	\$94.80
Systems Engineer - Cyber Security - (Junior)	Customer Facility	-	\$115.31	\$118.19
Systems Engineer - Cyber Security - (Intermediate)	Customer Facility	-	\$135.00	\$138.38
Systems Engineer - Cyber Security - (Senior)	Customer Facility	-	\$166.10	\$170.25
Cybersecurity System Administrator (Junior)	Customer Facility	-	\$87.26	\$89.44
Cybersecurity System Administrator (Intermediate)	Customer Facility	-	\$107.85	\$110.55

Labor Category	Contractor or Customer Facility or Both	10/16/2020 - 10/15/2021	10/16/2021 - 10/15/2022	10/16/2022 - 10/15/2023
Cybersecurity System Administrator (Senior)	Customer Facility	-	\$128.65	\$131.87
Cybersecurity Architect (Junior)	Customer Facility	-	\$97.59	\$100.03
Cybersecurity Architect (Intermediate)	Customer Facility	-	\$117.80	\$120.75
Cybersecurity Architect (Senior)	Customer Facility	-	\$188.03	\$192.73
Cybersecurity Engineer (Junior)	Customer Facility	-	\$97.59	\$100.03
Cybersecurity Engineer (Intermediate)	Customer Facility	-	\$139.62	\$143.11
Cybersecurity Engineer (Senior)	Customer Facility	-	\$157.59	\$161.53
Cyber Threat Analyst (Junior)	Customer Facility	-	\$80.75	\$82.77
Cyber Threat Analyst (Intermediate)	Customer Facility	-	\$88.16	\$90.36
Cyber Threat Analyst (Senior)	Customer Facility	-	\$123.08	\$126.16
Cybersecurity DevOps Engineer (Junior)	Customer Facility	-	\$93.84	\$96.19
Cybersecurity DevOps Engineer (Intermediate)	Customer Facility	-	\$121.67	\$124.71
Cybersecurity DevOps Engineer (Senior)	Customer Facility	-	\$155.11	\$158.99
Database Administrator - Cyber Security - (Junior)	Customer Facility	-	\$96.00	\$98.40
Database Administrator - Cyber Security - (Intermediate)	Customer Facility	-	\$150.51	\$154.27
Database Administrator - Cyber Security - (Senior)	Customer Facility	-	\$157.06	\$160.99
Cybersecurity Database Engineer (Junior)	Customer Facility	-	\$94.01	\$96.36
Cybersecurity Database Engineer (Intermediate)	Customer Facility	-	\$120.23	\$123.24
Cybersecurity Database Engineer (Senior)	Customer Facility	-	\$139.38	\$142.86
User Experience / User Interface Engineer (Junior)	Customer Facility	-	\$88.04	\$90.24

Labor Category	Contractor or Customer Facility or Both	10/16/2020 - 10/15/2021	10/16/2021 - 10/15/2022	10/16/2022 - 10/15/2023
User Experience / User Interface Engineer (Intermediate)	Customer Facility	-	\$108.75	\$111.47
User Experience / User Interface Engineer (Senior)	Customer Facility	-	\$128.44	\$131.65
Application Security SME / Lead (Junior)	Customer Facility	-	\$97.59	\$100.03
Application Security SME / Lead (Intermediate)	Customer Facility	-	\$117.80	\$120.75
Application Security SME / Lead (Senior)	Customer Facility	-	\$169.12	\$173.35
Cybersecurity Software Developer (Junior)	Customer Facility	-	\$93.84	\$96.19
Cybersecurity Software Developer (Intermediate)	Customer Facility	-	\$121.67	\$124.71
Cybersecurity Software Developer (Senior)	Customer Facility	-	\$135.94	\$139.34
Cybersecurity Information Assurance Engineer (Junior)	Customer Facility	-	\$88.02	\$90.22
Cybersecurity Information Assurance Engineer (Intermediate)	Customer Facility	-	\$111.56	\$114.35
Cybersecurity Information Assurance Engineer (Senior)	Customer Facility	-	\$137.86	\$141.31
Cybersecurity Incident Responder (Junior)	Customer Facility	-	\$97.59	\$100.03
Cybersecurity Incident Responder (Intermediate)	Customer Facility	-	\$117.80	\$120.75
Cybersecurity Incident Responder (Senior)	Customer Facility	-	\$139.62	\$143.11
Penetration Tester (Junior)	Customer Facility	-	\$95.21	\$97.59
Penetration Tester (Intermediate)	Customer Facility	-	\$136.22	\$139.63
Penetration Tester (Senior)	Customer Facility	-	\$153.75	\$157.59
Computer Forensics Analyst (Junior)	Customer Facility	-	\$106.85	\$109.52
Computer Forensics Analyst (Intermediate)	Customer Facility	-	\$121.55	\$124.59
Computer Forensics Analyst (Senior)	Customer Facility	-	\$139.62	\$143.11

Labor Category	Contractor or Customer Facility or Both	10/16/2020 - 10/15/2021	10/16/2021 - 10/15/2022	10/16/2022 - 10/15/2023
CLOUD Software Engineer - Mid	Both	-	\$132.59	\$135.91
CLOUD Software Engineer - Sr	Both	-	\$165.86	\$170.01
CLOUD System Engineering Expert	Both	-	\$171.25	\$175.53
CLOUD Software Engineer - Expert	Both	-	\$212.74	\$218.05
Administrative Assistant	Both	-	\$54.41	\$55.77

SCLS Matrix

SCLS Eligible Contract Labor Category/Fixed Price Service	SCLS Equivalent Code Title	WD Number
Administrative Assistant	01020 - Administrative Assistant	2015-4281

The Service Contract Labor Standards, formerly the Service Contract Act (SCA), apply to this contract and it includes SCLS applicable labor categories. Labor categories and fixed price services marked with a (**) in this pricelist are based on the U.S. Department of Labor Wage Determination Number(s) identified in the SCLS/SCA matrix. The prices awarded are in line with the geographic scope of the contract (i.e., nationwide).

GSA Software

ID Dataweb GSA Price List Prices are inclusive of Industrial Funding Fee (IFF)

SIN	Part Number	Product Description	GSA Price
511210	IDW-101-001-01	AXN Cloud-based Software Modules: Annual License fee plus per user fee for utilizing the AXN network and individual services. The AXN Core Service Module includes use of the AXN itself, including the Administrative Management Console, full access to the network of attribute providers, and help desk support. Requires a minimum purchase of \$3,000.00 per year (requires a minimum purchase of 12,000 credentials). Pricing is per-credential per year.	\$0.24
511210	IDW-102-001-01	AXN Cloud-based Software Modules: Annual License fee plus per user fee for utilizing the AXN network and individual services. The AXN Risk Score and Policy Service Module aggregates scores and signals from all selected attribute providers and converts to a single score from 0-100 to indicate trust. Organizations can map their own weights and values to the AXN Trust Score, enabling tailored scores directly reflecting the organization's compliance and risk requirements. In addition, organizations can map PASS, FAIL and STEP UP decisions to their transactions - simplifying workflow and policy. This module also enables the customer to create multi-step verification processes - triggering step ups and fallbacks depending on results. Requires a minimum purchase of \$6,000.00 per year (requires a minimum purchase of 12,000 credentials). Pricing is per-credential per year.	\$0.48
511210	IDW-103-001-01	AXN Cloud-based Software Modules: Annual License fee plus per user fee for utilizing the AXN network and individual services. The AXN Reporting, Compliance and Auditing Module allows top-down executive reporting, covering metrics, trends, and general analytics. In addition, Administrators have access to individual transaction details, including individual metrics and tests leading to decisions. Requires a minimum purchase of \$1,200.00 per year (requires a minimum purchase of 24,000 credentials). Pricing is per-credential per year.	\$0.05