APPROVED

General Services Administration
Federal Acquisition Service
Information Technology Schedule Pricelist
General Purpose Commercial Information Technology Equipment, Software, and Services

GS-35F-470CA

TENICA and Associates LLC
4795 Meadow Wood Lane, Suite 200W
Chantilly, VA 20151
Phone: (703) 955-7770
GSAinfo@tenica.biz
www.TENICA.biz

Contact for Contract Administration: Terry Scherling
GSAContracts@tenica.biz

Pricelist current through modification PA-0021, dated 9/6/2018

FEDERAL SUPPLY SERVICE
GENERAL PURPOSE COMMERCIAL INFORMATION TECHNOLOGY EQUIPMENT, SOFTWARE, AND SERVICES
SCHEDULE PRICELIST

General Description

TENICA and Associates, LLC was founded in 2008 and is based in Chantilly, Virginia. In 2016, TENICA acquired Polar Star Consulting LLC (PSC) and totally merged it into the TENICA organization. PSC had been providing a broad array of Information Technology (IT) services related to this schedule since its founding in 2006. In addition to providing IT services to large telecommunications providers and consulting groups, we have provided Contract Advisory and Assistance Services and IT Systems Engineering and Technical Assistance services as a subcontractor supporting US government contracts with the Defense Information Systems Agency and several agencies in the Intelligence Community.

Contract Number: *GS-35F-470CA*

Period Covered by Contract: *August 21, 2015 through August 20, 2020*

For more information on ordering from Federal Supply Schedules, click on the FSS Schedules button at http://fss.gsa.gov.

General Services Administration
Federal Supply Service

Online 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. Agencies can access GSA *Advantage!* via the Internet at http://www.GSAAdvantage.gov.

TABLE OF CONTENTS

1. CUSTOMER INFORMATION

1. Special Item Numbers (SIN):

a. Table of awarded SINs

SIN	FSC Class/ FPDS Code	Products/Services
132-51, 132-51STLOC, 132-51 RC Information Technology Professional Services, 132-45A, 132-45B, 132-45C, 132-45D IT Highly Adaptive Cybersecurity Services	FSC/PSC Class D308	Programming Services
	FSC/PSC Class D399	Other IT Services, Not Elsewhere Classified

b. Prices shown in the pricelist are net.

c. A description of all corresponding commercial job titles, experience, functional responsibility, and education for those types of employees or subcontractors who perform services is provided starting on page 9.

2. Maximum Order:

a. Orders exceeding the maximum order threshold may be placed in accordance with clause I-FSS-125, Requirements Exceeding the Maximum Order.

b. The Maximum Order value for the following SINs is $500,000.

132-51 132-51STLOC 132-51RC	IT Professional Services
132-45A	Penetration Testing
132-45B	Incident Response
132-45C	Cyber Hunt
132-45D	Risk and Vulnerability Assessments (RVA)

3. Minimum Order:

The Minimum Order for the following SINs is $100.00.

132-51 132-51STLOC 132-51RC	IT Professional Services
132-45A	Penetration Testing
132-45B	Incident Response
132-45C	Cyber Hunt
132-45D	Risk and Vulnerability Assessments (RVA)

4. **Geographic Coverage:** The geographic scope of contract is domestic and overseas delivery.

5. **Production Point:** Prices shown are NET prices; basic discounts have been deducted.

6. **Discounts:**

   a. Quantity – None

   b. Dollar Volume – None.

7. **Prompt Payment:** 0% - 10 days; 0% - Net 30

8. **Government Purchase Cards:**

   a. Contractors are required to accept credit cards for payments equal to or less than the micro-purchase threshold for oral or written delivery orders.

   b. Credit cards are not acceptable for payment above the micro-purchase threshold. In addition, bank account information for wire transfer payments will be shown on the invoice.

9. **Foreign Items:** Not applicable.

10. **Delivery Schedule:**

    a. TIME OF DELIVERY: The Contractor shall deliver to destination within the number of calendar days after receipt of order (ARO), as set forth below:

Special Item Numbers	**Delivery Time (Days ARO)**
SIN 132-51, 132-45A, 132-45B 132-45C, 132-45D	TBD between TENICA and the ordering activity

    b. EXPEDITED DELIVERY: As negotiated between TENICA and ordering activity.

    c. OVERNIGHT and TWO-DAY DELIVERY: As negotiated between TENICA and ordering activity.

d. URGENT REQUIREMENTS: When the Federal Acquisition Schedule contract delivery period does not meet the bona fide urgent delivery requirements of an ordering activity, ordering activities are encouraged, if time permits, to contact the contractor for the purpose of obtaining accelerated delivery. The contractor shall reply to the inquiry within three workdays after receipt. (Telephonic replies shall be confirmed by the Contractor in writing.) If the contractor offers an accelerated delivery time acceptable to the ordering activity, any order(s) placed pursuant to the agreed upon accelerated delivery time frame shall be delivered within this shorter delivery time and in accordance with all other terms and conditions of the contract.

11. **FOB:** Destination

12. **Ordering Information**

a. Agencies should address all orders to the following address:

TENICA and Associates, LLC
4795 Meadow Wood Lane, Suite 200W
Chantilly, Virginia 20151

b. For supplies and services, the order procedures, information on Blanket Purchase Agreements (BPA) are found in Federal Acquisition Regulation (FAR) 8.405-3.

13. **Payment Information:**

a. Agencies should address all payments to the following address:

TENICA and Associates, LLC
4795 Meadow Wood Lane, Suite 200W
Chantilly, Virginia 20151

b. The contact information to obtain technical and/or ordering assistance is:

703.955.7770
GSAinfo@TENICA.biz

14. **Warranty Provision:** Standard Commercial Warranty.

15. **Statement Concerning Availability of Export Packing:** Not applicable.

16. **Terms and Conditions of Government Purchase Card Acceptance Above the Micropurchase Threshold:** Not applicable.

17. **Terms and Conditions of Rental, Maintenance, and Repair:** Not applicable.

18. **Terms and Conditions of Installation:** Not applicable.

19. **Terms and Conditions of Repair Parts Indicating Date of Parts Price Lists and any Discounts from List Prices:** Not applicable.

20. **Terms and Conditions for Any Other Services:** Not applicable.

21. **Service and Distribution Points:** Not applicable.

22. **Participating Dealers:** Not applicable.

23. **Preventive Maintenance:** Not applicable.

24. **Environmental Attributes:** None

25. **Section 508 Compliance:** In accordance with Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), FAR 39.2, and the Architectural and Transportation Barriers Compliance Board Electronic and Information Technology (EIT) Accessibility Standards (36 CFR 1194) General Services Administration (GSA), where applicable, all items and services offered under the contract are 508 compliant.

    ☒ Yes
    ☐ No

    Section 508 compliance information on the supplies and services in this contract are available at the following: 703-955-7770; GSAinfo@TENICA.biz

    The EIT standard can be found at: http://www.section508.gov/.

26. **Data Universal Numbering System (DUNS) Number:** 805618639

27. Contractor **HAS** registered with the System for Award Management (SAM).

2. TERMS AND CONDITIONS APPLICABLE TO IT PROFESSIONAL SERVICES (SIN 132-51) AND IT HIGHLY ADAPTIVE CYBERSECURITY SERVICES (SINS 132-45A, 132-45B, 132-45C AND 132-45D)

1. Scope

a. The prices, terms, and conditions stated under SIN 132-51 IT Professional Services apply exclusively to IT Services within the scope of this IT Schedule.

b. The prices, terms, and conditions stated under SINs 132-45A, 132-45B, 132-45C and 132-45D IT Highly Adaptive Cybersecurity Services apply exclusively to Cyber Services within the scope of this IT Schedule.

c. 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** I-FSS-60 Performance Incentives (April 2000)

a. Performance incentives may be agreed upon between the contractor and the ordering activity on individual fixed price orders or BPAs.

b. The ordering activity must establish a maximum performance incentive price for these services and/or total solutions on individual orders or BPAs.

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, Electronic Data Interchange (EDI) orders, BPAs, individual purchase orders, or task orders for ordering services under this contract. BPAs 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 that 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 52.232-15) (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 order 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

In accordance with FAR 52.21404 Contract Terms and Conditions Commercial Items (Mar 2009) (Deviation I – Feb 2007) for firm-fixed price orders and FAR 52.212-4 Contract Terms and Conditions Commercial Items (Mar 2009) (Alternate I – Oct 2008) (Deviation I – Feb 2007) applies to time-and-materials and labor-hour contracts 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 – Dec 2007) 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 Professional Services.

9. Independent Contractor

All IT Professional 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, consultants, 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 contractor, 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 that may require restrictions are provided at FAR 9.508.

11. Invoices

The contractor, upon completion of the work ordered, shall submit invoices for IT Professional 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 52.212.-4 (Mar 2009) (Alternate I – Oct 2008) (Deviation I – Feb 2007) 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 52.212-4 (Mar 2009) (Alternate I – Oct 2008) (Deviation I – Feb 2007) 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. Résumés

Résumés 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 written consent from the ordering activity's Contracting Officer before placing any subcontract for furnishing any of the work called for in a task order.

16. Descrption of Labor Categories

Job Titles	Functional Responsibilities	Minimum Education and Experience
Program Manager 6	Minimum of 25 years' experience as a program/project manager (or experience in related disciplines) for complex and large-dollar systems. Requires formal government or commercial training and/or certification in program/project management disciplines including cost/budget management, schedule management, meeting system technical performance requirements, and risk management. Requires management of other program/project managers to deliver integrated end solutions.	Bachelor's degree, 25 years' experience
Program Manager 5	Minimum of 20 years' experience as a program/project manager (or experience in related disciplines) for complex and large-dollar systems. Requires some formal government or commercial training and/or certification in program/project management disciplines including cost/budget management, schedule management, meeting system technical performance requirements, and risk management. Typically requires management of other program/project managers to deliver integrated end solutions.	Bachelor's degree, 20 years' experience
Program Manager 4	Minimum of 15 years' experience as a program/project manager (or experience in related disciplines) for complex and large-dollar systems. Requires some formal government or commercial training and/or certification in program/project management disciplines including cost/budget management, schedule management, meeting system technical performance requirements, and risk management.	Bachelor's degree, 15 years' experience
Program Manager 3	Minimum of 10 years' experience as a program/project manager (or experience in related disciplines) for complex and large-dollar systems. Disciplines include cost/budget management, schedule management, meeting system technical performance requirements, and risk management.	Bachelor's degree, 10 years' experience
Telecommunications Subject-Matter Expert (SME)/Scientist 6	Minimum 25 years' experience as an engineer or scientist in one or more of the disciplines of computer science, computer or electrical engineering or related sub-disciplines. Duties typically involve performing scientific or engineering services that may include but are not limited to: engineering studies and analyses; technology planning; systems architecture development; requirements development; concept development; systems design; system development and integration; test and evaluation; systems operation; construction; control of systems and components; integrated logistics support; modeling and simulation; configuration management; and systems acquisition and lifecycle management in compliance with current industry and government practices. Recognized authority within field of expertise and extensive knowledge of related fields.	Bachelor's degree, 25 years' experience
Telecommunications SME/Scientist 5	Minimum 20 years' experience as an engineer or scientist in one or more of the disciplines of computer science, computer or electrical engineering or related sub-disciplines. Duties typically involve	Bachelor's degree,

Job Titles	Functional Responsibilities	Minimum Education and Experience
	performing scientific or engineering services that may include but are not limited to: engineering studies and analyses; technology planning; systems architecture development; requirements development; concept development; systems design; system development and integration; test and evaluation; systems operation; construction; control of systems and components; integrated logistics support; modeling and simulation; configuration management; and systems acquisition and lifecycle management in compliance with current industry and government practices. Recognized authority within field of expertise and extensive knowledge of related fields.	20 years' experience
Telecommunications SME/Scientist 4	Minimum 15 years' experience as an engineer or scientist in telecommunications or one or more of the disciplines of computer science, systems, chemical, civil, electrical, or mechanical engineering or related sub-disciplines. Duties typically involve performing scientific or engineering services that may include but are not limited to: engineering studies and analyses; technology planning; systems architecture development; requirements development; concept development; systems design; system development and integration; test and evaluation; systems operation; construction; control of systems and components; integrated logistics support; modeling and simulation; configuration management; and systems acquisition and lifecycle management in compliance with current industry and government practices.	Bachelor's degree, 15 years' experience
Telecommunications SME/Scientist 3	Minimum 10 years' experience as an engineer or scientist in telecommunications or one or more of the disciplines of computer science, systems, chemical, civil, electrical, or mechanical engineering or related sub-disciplines. Duties typically involve performing scientific or engineering services that may include but are not limited to: engineering studies and analyses; technology planning; systems architecture development; requirements development; concept development; systems design; system development and integration; test and evaluation; systems operation; construction; control of systems and components; integrated logistics support; modeling and simulation; configuration management; and systems acquisition and lifecycle management in compliance with current industry and government practices.	Bachelor's degree, 10 years' experience
Network Engineer 5	Minimum 20 years' experience in a disciplined branch of engineering. Strong working knowledge in one or more of the following disciplines: systems engineering, electrical engineering, civil engineering/architecture, optical engineering, materials science & engineering, reliability and maintainability (R&M) engineering, quality engineering, and test engineering.	Bachelor's degree, 20 years' experience
Network Engineer 4	Minimum 15 years' experience in a disciplined branch of telecommunications or engineering. Strong working knowledge in one or more of the following disciplines: systems engineering, electrical engineering, quality engineering, and test engineering.	Bachelor's degree, 15 years' experience
Network Engineer 3	Minimum 10 years' experience in a disciplined branch of engineering. Strong working knowledge in one or more of the following disciplines: systems engineering, electrical engineering, quality engineering, and test engineering.	Bachelor's degree, 10 years' experience
Network Engineer 2	Minimum 5 years' experience in a disciplined branch of engineering. Strong working knowledge in one or more of the following	Bachelor's degree,

Job Titles	Functional Responsibilities	Minimum Education and Experience
	disciplines: systems engineering, electrical engineering, quality engineering, and test engineering.	5 years' experience
Network Engineer 1	New entrant to the area of network engineering. Strong working knowledge in one or more of the following disciplines: systems engineering, electrical engineering, quality engineering, and test engineering.	Bachelor's degree, <5 years' experience
Network Solutions Architect 5	Minimum 20 years' experience in a disciplined branch of engineering developing complex system architectures, planning, design, development, evaluation, and operation of IT systems. Duties typically involve performing engineering services that may include but are not limited to: engineering studies and analyses; technology planning; systems architecture development; requirements development; concept development; systems design; system development and integration; test and evaluation; systems operation; construction; control of systems and components; integrated logistics support; modeling and simulation; configuration management; and systems acquisition and lifecycle management in compliance with current industry and government practices.	Bachelor's degree, 20 years' experience
Network Solutions Architect 4	Minimum 15 years' experience in a disciplined branch of engineering planning, design, development, evaluation, and operation of IT systems. Able to define changes to a complex IT system and provide direct implementation support. Provides integration support for application deployment of complex, multi-server and distributed systems. Ability to derive requirements from Statements of Objectives and translate them into activities related to the operations of a complex system.	Bachelor's degree, 15 years' experience
Network Solutions Architect 3	Minimum 10 years' experience planning, design, development, evaluation, and operation of IT systems. Able to derive requirements from Statements of Objectives and translate them into activities related to the operations of a complex system.	Bachelor's degree, 10 years' experience
Network Solutions Architect 2	Minimum 5 years' experience planning, design, development, evaluation, and operation of IT systems. Able to derive requirements from Statements of Objectives and translate them into activities related to the operations of a complex system.	Bachelor's degree, 5 years' experience
Network Solutions Architect 1	New entrant to the area of planning, design, development, evaluation, and operation of IT systems. Able to derive requirements from Statements of Objectives and translate them into activities related to the operations of a complex system.	Bachelor's degree, <5 years' experience
Systems Architect 5	Minimum 20 years' experience in managing and implementing large, complex IT systems to meet business objectives. Analyzes, designs, tests, and evaluates new or existing systems. Assesses the feasibility, cost, and practicality of implementing new or converting existing systems against developing new technology. Develops detailed system architecture or conversion plans to define the conversion process, environmental considerations, and system constraints.	Bachelor's degree, 20 years' experience
Systems Architect 4	Minimum 15 years' experience in managing and implementing large, complex IT systems to meet business objectives. Analyzes, designs, tests, and evaluates new or existing systems. Assesses the feasibility, cost, and practicality of implementing new or converting existing systems against developing new technology. Develops detailed system architecture or conversion plans to define the conversion process, environmental considerations, and system constraints.	Bachelor's degree, 15 years' experience

Job Titles	Functional Responsibilities	Minimum Education and Experience
Systems Architect 3	Minimum 10 years' experience in managing and implementing large, complex IT systems to meet business objectives. Analyzes, designs, tests, and evaluates new or existing systems. Assesses the feasibility, cost, and practicality of implementing new or converting existing systems against developing new technology. Develops detailed system architecture or conversion plans to define the conversion process, environmental considerations, and system constraints.	Bachelor's degree, 10 years' experience
Systems Architect 2	Minimum 5 years' experience in managing and implementing large, complex IT systems to meet business objectives. Analyzes, designs, tests, and evaluates new or existing systems. Assesses the feasibility, cost, and practicality of implementing new or converting existing systems against developing new technology. Develops system architecture or conversion plans to define the conversion process, environmental considerations, and system constraints.	Bachelor's degree, 5 years' experience
Systems Architect 1	New entrant to the area of implementing IT systems to meet business objectives. Able to analyze, design, test, and evaluate new or existing systems. Able to assist with developing system architecture or conversion plans to define the conversion process, environmental considerations, and system constraints.	Bachelor's degree, <5 years' experience
Systems Engineer 5	Minimum 20 years' experience in establishing integrated system-level requirements for an overall information, technical, and data architecture in support of multiple software applications. Performs platform capability analyses and evaluations, selects components, and develops system and LAN interfaces to ensure compliance with requirements. Constructs models and simulations of computer systems to demonstrate ability to meet user requirements. Executes system stress tests to identify software performance constraints; tunes application and operating system software to enhance performance accordingly.	Bachelor's degree, 20 years' experience
Systems Engineer 4	Minimum 15 years' experience in establishing integrated system-level requirements for an overall information, technical, and data architecture in support of multiple software applications. Performs platform capability analyses and evaluations, selects components, and develops system and LAN interfaces to ensure compliance with requirements. Constructs models and simulations of computer systems to demonstrate ability to meet user requirements. Executes system stress tests to identify software performance constraints; tunes application and operating system software to enhance performance accordingly.	Bachelor's degree, 15 years' experience
Systems Engineer 3	Minimum 10 years' experience in establishing integrated system-level requirements for an overall information, technical, and data architecture in support of multiple software applications. Performs platform capability analyses and evaluations, selects components, and develops system and LAN interfaces to ensure compliance with requirements. Constructs models and simulations of computer systems to demonstrate ability to meet user requirements. Executes system stress tests to identify software performance constraints; tunes application and operating system software to enhance performance accordingly.	Bachelor's degree, 10 years' experience
Systems Engineer 2	Minimum 5 years' experience in establishing integrated system-level requirements for an overall information, technical, and data architecture in support of multiple software applications. Performs	Bachelor's degree,

Job Titles	Functional Responsibilities	Minimum Education and Experience
	platform capability analyses and evaluations, selects components, and develops system and LAN interfaces to ensure compliance with requirements. Constructs models and simulations of computer systems to demonstrate ability to meet user requirements. Executes system stress tests to identify software performance constraints; tunes application and operating system software to enhance performance accordingly.	5 years' experience
Systems Engineer 1	New entrant to the area of establishing integrated system-level requirements for overall information, technical, and data architecture in support of multiple software applications. Performs platform capability analyses and evaluations, selects components, and develops system and LAN interfaces to ensure compliance with requirements. Assists in constructing models and simulations of computer systems to demonstrate ability to meet user requirements. Assists in executing system stress tests to identify software performance constraints; tunes application and operating system software to enhance performance accordingly.	Bachelor's degree, <5 years' experience
Systems Integrator 5	Minimum 20 years' experience managing work for technical program offices that requires integration of program/system information and execution across multiple programs/projects/ systems. Possesses a combination of leadership, management, and technical expertise within the types of programs being integrated. Can manage other systems integrators.	Bachelor's degree, 20 years' experience
Systems Integrator 4	Minimum 15 years' experience managing work for technical program offices that requires integration of program/system information and execution across multiple programs/projects/ systems. Possesses a combination of leadership, management, and technical expertise within the types of programs being integrated. Can manage other systems integrators.	Bachelor's degree, 15 years' experience
Systems Integrator 3	Minimum 10 years' experience managing work for technical program offices that requires integration of program/system information and execution across multiple programs/projects/ systems. Possesses a combination of leadership, management, and technical expertise within the types of programs being integrated.	Bachelor's degree, 10 years' experience
Systems Integrator 2	Minimum 5 years' experience managing work for technical program offices that requires integration of program/system information and execution across multiple programs/projects/ systems.	Bachelor's degree, 5 years' experience
Systems Integrator 1	New entrant to the area of managing work for technical program offices that require integration of program/system information and execution across multiple programs/projects/systems.	Bachelor's degree, <5 years' experience
BPI / Ops Research SME 5	Minimum 20 years' experience and acknowledged as a SME within the occupation and/or specific skill. Certified with the specific language, system, process, or technology. For specific computer languages, systems, processes, or technologies, expertise with the subject matter or technology outweighs the number of years of experience.	Bachelor's degree, 20 years' experience
BPI / Ops Research SME 4	Minimum 15 years' experience and acknowledged as a SME within the occupation and/or specific skill. Certified with the specific language, system, process, or technology. For specific computer languages, systems, processes, or technologies, expertise with the	Bachelor's degree, 15 years' experience

Job Titles	Functional Responsibilities	Minimum Education and Experience
	subject matter or technology outweighs the number of years of experience.	
BPI / Ops Research SME 3	Minimum 10 years' experience and acknowledged as a SME within the occupation and/or specific skill. Certified with the specific language, system, process, or technology. For specific computer languages, systems, processes, or technologies, expertise with the subject matter or technology outweighs the number of years of experience.	Bachelor's degree, 10 years' experience
Vulnerability Assessment Analyst and Penetration Tester 1	May support in part or in whole technical vulnerability assessments of applications and infrastructure, vulnerability research, and generation of assessment reports. Duties may include: • Executing tests by following the steps and procedures listed in a test plan and documenting results in a standardized format that is appropriate for future analyses • Assisting in the coordination of technical tests, network scans, and/or vulnerability scans that support the evaluation of information safeguard effectiveness • Conducting reconnaissance data gathering and vulnerability research • Assisting in the creation of risk and vulnerability reporting	Bachelor's degree
Vulnerability Assessment Analyst and Penetration Tester 2	May support in part or in whole technical vulnerability assessments of applications and infrastructure, vulnerability research, and generation of assessment reports. Duties may include: • Supporting development of and following general test and evaluation plans to compare current and proposed technologies; assessing test results to determine whether they match requirements specifications • Assisting in the coordination of technical tests, network scans, and/or vulnerability scans that support the evaluation of information safeguard effectiveness • Conducting reconnaissance, target assessment, data gathering, and vulnerability research • Leveraging COTS tools to conduct vulnerability assessments, analyzing results, identifying exploitable vulnerabilities, and verifying vulnerabilities • Preparing report documents by tailoring technical information and creating benchmark or security authorization reports; outlining key findings related to speed, risks, results and reliability, and recommending acceptance or rejection of technology for applied use	Bachelor's degree, 3 years' experience
Vulnerability Assessment Analyst and Penetration Tester 3	May support in part or in whole technical vulnerability assessments of applications and infrastructure, vulnerability research, and generation of assessment reports. Duties may include: • Contributing to the selection of appropriate technical tests, network or vulnerability scan tools, and/or pen testing tools based on review of requirements and purpose; listing all steps involved for executing selected test(s) and coaching others in the use of advanced research, development, or scan tools and the analysis of comparative findings between proposed and current technologies • Coordinating or leading teams to conduct ethical tests, network scans, and/or vulnerability scans that support the evaluation of information safeguard effectiveness • Conducting reconnaissance, target assessment, target selection, and vulnerability research • Using COTS tools, conducting or leading teams to conduct vulnerability assessments, analyzing results, identifying exploitable	Bachelor's degree, 5 years' experience

Job Titles	Functional Responsibilities	Minimum Education and Experience
	vulnerabilities, and verifying vulnerabilities through manual assessment • Preparing and reviewing assessment documents, validating and communicating key findings to stakeholders	
Vulnerability Assessment Analyst and Penetration Tester 4	May support in part or in whole technical vulnerability assessments of applications and infrastructure, vulnerability research, and generation of assessment reports. Duties may include: • Devising and/or selecting appropriate technical tests, network or vulnerability scan tools, and/or pen testing tools based on review of requirements and purpose; listing all steps involved for executing selected test(s) and coaching others in the use of advanced research, development, or scan tools and the analysis of comparative findings between proposed and current technologies • Coordinating or leading teams to conduct ethical tests, network scans, and/or vulnerability scans that support the evaluation of information safeguard effectiveness • Conducting reconnaissance, target assessment, target selection, and vulnerability research • Creating custom tools and exploits to penetrate various levels of controls including network, operating system, and physical • Using COTS or custom tools, conducting or leading teams to conduct vulnerability assessments, analyzing results, identifying exploitable vulnerabilities, and verifying vulnerabilities through manual assessment • Preparing and reviewing assessment documents, validating and communicating key findings to stakeholders	Bachelor's degree, 6 years' experience
Incident Response Analyst 1	Contributes to generating response to crisis or urgent situations to mitigate immediate or potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Duties may include: • Handling and responding to cyber security incidents through coordination with stakeholders such as internal IT entities, security leadership, legal affairs, internal affairs, law enforcement, and privacy offices • Receiving incident reporting, conducting ticket updates, and notifying stakeholders of cyber security incidents and forensic investigations in relation to computer security incidents and escalate when necessary as well as coordinating response to computer security incidents • Recommending a course of action on each incident and creating, managing, and recording all actions taken; serving as initial POC for Events of Interest reported both internally and externally • Establishing alarm/incident escalation process and tracking, following up, and resolving incidents • Initiating and maintaining contact with affected parties during incident response lifecycle; investigating potential incidents/intrusions	Bachelor's degree
Incident Response Analyst 2	Contributes to generating responses to crisis or urgent situations to mitigate immediate and / or potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Duties may include:	Bachelor's degree, 2 years' experience

Job Titles	Functional Responsibilities	Minimum Education and Experience
	• Providing oversight for incident data flow and response, content, and remediation, and partnering with other incident response centers in maintaining an understanding of threats, vulnerabilities, and exploits that could impact networks and assets • Performing real-time proactive event investigation on various security enforcement systems, such as SIEM, anti-virus, internet content filtering/reporting, malcode prevention, firewalls, IDS & IPS, web security, anti-spam, etc. • Performing the role of Incident Coordinator for IT security events requiring focused response, containment, investigation, and remediation • Performing forensic analysis on hosts supporting investigations • Conducting malware analysis in out-of-band environment (static and dynamic), including complex malware	
Incident Response Analyst 3	Contributes to generating responses to crisis or urgent situations to mitigate immediate and / or potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Duties may include: • Leading shifts and functional IR teams, providing oversight for incident data flow and response, content, and remediation, and partnering with other incident response centers in maintaining an understanding of threats, vulnerabilities, and exploits that could impact networks and assets • Performing real-time proactive event investigation on various security enforcement systems, such as SIEM, anti-virus, internet content filtering/reporting, malcode prevention, firewalls, IDS & IPS, web security, anti-spam, etc. • Performing the role of Incident Coordinator for IT security events requiring focused response, containment, investigation, and remediation • Performing forensic analysis on hosts supporting investigations • Conducting malware analysis in out-of-band environment (static and dynamic), including complex malware • Coordinating response action to identifies threats and incidents • Analyzing operational anomalies and network behavior, performing mitigation cyber threat monitoring and anomaly analysis, and actively monitoring the networks for cybersecurity threats and vulnerabilities • Providing oversight and perform quality assurance on incident closures • Assisting with knowledge management - Standard Operating Procedures (SOP) and procedural support data	Bachelor's degree, 5 years' experience
Incident Response Analyst 4	Contributes to generating responses to crises or urgent situations to mitigate immediate and/or potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Duties may include: • Leading one or more functional security teams (incident response, forensics, cyber intelligence etc.) • Supporting the development of staff schedules and staffing forecasts for approval • Ensuring that shift members follow the appropriate incident escalation and reporting procedures	Bachelor's degree, 7 years' experience

Job Titles	Functional Responsibilities	Minimum Education and Experience
	• Providing support promptly and efficiently through front-line telephone and email communications • Ingesting, triaging, prioritizing, assigning, tracking, documenting, and managing incidents and results • Providing technical support in response to computer security incidents • Correlating, mapping, and fusing any and all incident information for the development and distribution of cyber alerts and notices, or other products as required • Documenting technical details of current or potential intruder threats consistent with environment • Coordinating, communicating, sharing information, and working closely with organizational stakeholders • Bearing responsibility for knowledge management of operational procedures and support documentation	
Security Operations Center (SOC) Analyst 1	Provides cyber threat analysis and reporting to support SOC and Program situational awareness. Actively monitors security threats and risks, tracks investigation results, and reports on findings. Duties may include: • Supporting Security Operations Center, monitoring security tools to review and analyze pre-defined events indicative of incidents, and providing first-tier response to security incidents • Following SOPs for detecting, classifying, and reporting incidents under the supervision of Tier 2 and Tier 3 staff • Managing cases within incident management systems	Bachelor's degree
Security Operations Center (SOC) Analyst 2	Provides cyber threat analysis and reporting to support SOC and program situational awareness. Actively monitors security threats and risks. Tracks investigation results and reports on findings. Duties may include: • Supporting Security Operations Center, monitoring security tools to review and analyze pre-defined events indicative of incidents, and providing first-tier response to security incidents • Monitoring network traffic for security events and performing triage analysis to identify security incidents • Responding to computer security incidents by collecting, analyzing, preserving digital evidence, and ensuring that incidents are recorded and tracked in accordance with SOC requirements • Working closely with the other teams to assess risk and provide recommendations for improving security posture • Recommending content to detect security events • Managing cases within incident management systems • Performing network forensics and deep packet analysis • Identifying countermeasures to detect and prevent security incidents	Bachelor's degree, 2 years' experience
Security Operations Center (SOC) Analyst 3	Provides cyber threat analysis and reporting to support SOC and program situational awareness. Actively monitors security threats and risks. Tracks investigation results and reports on findings. Duties may include: • Supporting a Security Operations Center, monitoring security tools to review and analyze pre-defined events indicative of incidents, and providing first-tier response to security incidents • Leading shifts and functional IR teams, providing oversight and bearing responsibility for event investigation and tracking activities	Bachelor's degree, 5 years' experience

Job Titles	Functional Responsibilities	Minimum Education and Experience
	• Supporting Tier 2 operations by monitoring alerts during critical and high-volume events • Conducting more in-depth analyses of security incidents to identify incidents of compromise • Performing intrusion scope and root cause analyses and assisting with intrusion remediation, strategy development, and implementation; recommending effective process changes to enhance defense and response procedures • Using SOC monitoring devices to review and analyze pre-defined events indicative of incidents; creating and recommending content to detect security events • Conducting malware analysis in out-of-band environments (static and dynamic), including complex malware • Vetting IOCs and conducting intelligence vetting and disposition, assessing feed viability • Performing network forensics and deep packet analysis • Identifying countermeasures to detect and prevent security incidents • Supporting knowledge management and developing procedures and policies for initial stand-up of a SOC	
Security Operations Center (SOC) Analyst 4	Provides cyber threat analysis and reporting to support SOC and program situational awareness. Actively monitors security threats and risks, provides in-depth incident analysis, evaluates security incidents, and provides proactive threat research. Tracks investigation results and reports on findings. Duties may include: • Leading multiple functional security teams, providing management and leadership of SOC • Using knowledge of regulatory compliance directives to include various monitoring and reporting requirements and industry best practices; implementing optimal workflows and procedures • Managing and ensuring the timely response and investigations of security events and incidents by the security operations center • Creating and maintaining schedules to ensure coverage by operations support personnel • Coordinating with threat operations and threat intelligence specialists to resolve high or critical severity level incidents • Bearing responsibility for knowledge management and developing procedures and policies for initial stand-up of a SOC	Bachelor's degree, 7 years' experience
Cyber Hunter 1	May respond to crises or urgent situations to mitigate immediate and potential threats. Approaches may include the use of information and threat intelligence specifically focused on a proximate incident to identify undiscovered attacks. Investigates and analyzes all relevant response activities. May identify and assesses the capabilities and activities of cyber criminals or foreign intelligence entities; designs and administers procedures in the organization that sustain the security of the organization's data and access to its technology and communications systems. Duties may include: • Utilizing various government and commercial resources to research known malware and attacks, define their characteristics, and report findings and mitigation recommendations to appropriate personnel • Using prescribed methods and materials to review and analyze events indicative of incidents • Attempting to detect the full spectrum of known cyber-attacks (e.g., DDoS, malware, phishing)	Bachelor's degree

Job Titles	Functional Responsibilities	Minimum Education and Experience
	• Pinpointing location of compromised systems and devices; correlating events from the various components in the IT security infrastructure and identifying attacks and breaches	
Cyber Hunter 2	May respond to crises or urgent situations to mitigate immediate and potential threats. Approaches may include the use information and threat intelligence specifically focused on a proximate incident to identify undiscovered attacks. Investigates and analyzes all relevant response activities. Identifies and assesses the capabilities and activities of cyber criminals or foreign intelligence entities; designs and administers procedures in the organization that sustain the security of the organization's data and access to its technology and communications systems. Duties may include: • Using current hashing algorithms to validate forensic images; diagramming networks and imaging servers to support digital forensics operations • Utilizing a variety of industry-standard tools and techniques to collect a system's current-state data and catalog, document, extract, collect, and preserve information • Using dynamic analysis to identify network intrusions and network monitoring tools to capture real-time traffic spawned by any running malicious code; identifying internet activity that is triggered by malware; identifying network/host-based characteristics and assisting in drafting recommendations to detect and prevent malware infections in the future • Monitoring and assessing complex security devices for patterns and anomalies (IDS, DLP); tagging events for Tier 1 monitoring • Pinpointing location of compromised systems and devices; correlating events from the various components in the IT security infrastructure and identifying attacks and breaches	Bachelor's degree, 4 years' experience
Cyber Hunter 3	May respond to crises or urgent situations to mitigate immediate and potential threats. Approaches may include the use information and threat intelligence specifically focused on a proximate incident to identify undiscovered attacks. Investigates and analyzes all relevant response activities. Identifies and assesses the capabilities and activities of cyber criminals or foreign intelligence entities; designs and administers procedures in the organization that sustain the security of the organization's data and access to its technology and communications systems. Duties may include: • Identifying, deterring, monitoring, and investigating computer and network intrusions • Providing computer forensic support to high technology investigations in the form of evidence seizure, computer forensic analysis, and data recovery • Monitoring and assessing complex security devices for patterns and anomalies from raw events (DNS, DHCP, AD, SE logs); tagging events for Tier 1 and 2 monitoring • Conducting malware analysis in out-of-band environments (static and dynamic), including complex malware	Bachelor's degree, 7 years' experience
Cyber Hunter 4	May respond to crises or urgent situations to mitigate immediate and potential threats. Approaches may include the use information and threat intelligence specifically focused on a proximate incident to identify undiscovered attacks. Investigates and analyzes all relevant response activities. Identifies and assesses the capabilities and	Bachelor's degree, 10 years' experience

Job Titles	Functional Responsibilities	Minimum Education and Experience
	activities of cyber criminals or foreign intelligence entities; designs and administers procedures in the organization that sustain the security of the organization's data and access to its technology and communications systems. Duties may include: • Leading Cyber Hunt team, providing oversight, and bearing responsibility for event investigation and tracking activities • Identifying, deterring, monitoring, and investigating computer and network intrusions • Providing computer forensic support to high technology investigations in the form of evidence seizure, computer forensic analysis, and data recovery • Monitoring and assessing complex security devices for patterns and anomalies from raw events (DNS, DHCP, AD, SE logs); tagging events for Tier 1 and 2 monitoring • Conducting malware analysis in out-of-band environments (static and dynamic), including complex malware	
Risk and Vulnerability Threat Analyst 1	Participates in conduct of controls and security assessments to assess risk of exposure of proprietary data through weaknesses in platforms, access procedures, or forms of access to the organization's systems and the data contained in them. Duties may include: • Providing technical support on post-event network security logs and trend analysis • Uncovering security and compliance violations • Associating and correlating IP address-related events with specific systems or devices in the IT infrastructure • Supporting development and analysis of system and security documentation • Maintaining documentation for exceptions to standards	Bachelor's degree
Risk and Vulnerability Threat Analyst 2	Participates in the conduct of controls and security assessments to assess risk of exposure of proprietary data through weaknesses in platforms, access procedures, or forms of access to the organization's systems and the data contained in them. Duties may include: • Developing, documenting, and executing containment strategies • Documenting and briefing the business on remediation options and executing the plan with stakeholders • Producing final reports and recommendations • Coordinating efforts of—and providing timely updates to—multiple business units during response • Performing in-depth analysis in support of incident response operations • Developing requirements for technical capabilities for cyber incident management • Investigating major breaches of security and recommending appropriate control improvements • Working with infrastructure and application support teams to drive closure of follow up actions identified through incident and problem management • Performing Security Control Assessments on systems to validate the results of risk assessments and ensure that controls in the security plan are present and operating correctly on the system; providing thorough report of the risks to the system and its data • Developing and analyzing system and security documentation	Bachelor's degree, 4 years' experience

Job Titles	Functional Responsibilities	Minimum Education and Experience
Risk and Vulnerability Threat Analyst 3	Participates in the conduct of controls and security assessments to assess risk of exposure of proprietary data through weaknesses in platforms, access procedures, or forms of access to the organization's systems and the data contained in them. Duties may include: • Supporting engineering design teams by assessing network and system security design features and making recommendations concerning overall security accreditation readiness and compliance and best practices • Supporting interoperability assessment teams and presenting written analyses and conclusions in all phases of analysis • Developing and analyzing system and security documentation • Following up with site administrators for status on non-compliant platforms and maintaining any necessary exception documentation • Maintaining documentation for exceptions to standards • Participating in Security Control Assessments on systems to validate the results of risk assessments and ensure that controls in the security plan are present and operating correctly on the system; providing thorough reports of the risks to the system and its data • Evaluating system findings, developing PO&AMs, and briefing stakeholders on key findings, recommendations, risk, and impact	Bachelor's degree, 7 years' experience
Risk and Vulnerability Threat Analyst 4	Participates in the conduct of controls and security assessments to assess risk of exposure of proprietary data through weaknesses in platforms, access procedures, or forms of access to the organization's systems and the data contained in them. Duties may include: • Being able to actively lead and manage project update briefings, working sessions, and stakeholder meetings • Applying strong analytical/assessment to security systems and enterprise architecture (e.g., conducting gap analyses, risk assessments) • Participating in Security Control Assessments on systems to validate the results of risk assessments and ensure that controls in the security plan are present and operating correctly on the system; providing thorough reports of the risks to the system and its data • Evaluating system findings, developing PO&AMs, and briefing stakeholders on key findings, recommendations, risk, and impact	Bachelor's degree, 10 years' experience
Cyber Security Engineer 1	Participates in special projects or investigations into specific technology or solution issues and research and piloting of new technologies. Serves as a point of contact for engineering efforts while assisting in maintaining compliance with the customer's policies and guidelines. Duties may include: • Providing administrative support to enterprise security devices • Providing support of various applications and implementing security standards • Assisting with configuration, validating secure complex systems, and testing security products and systems to detect security weaknesses	Bachelor's degree
Cyber Security Engineer 2	Participates in special projects or investigations into specific technology or solution issues and research and piloting of new technologies. Serves as a point of contact for engineering efforts while assisting in maintaining compliance with the customer's policies and guidelines. Duties may include: • Assisting with assessing, designing, developing, and recommending integrated security system solutions that ensure that proprietary and confidential data and systems are protected	Bachelor's degree, 3 years' experience

Job Titles	Functional Responsibilities	Minimum Education and Experience
	• Providing assistance with technical engineering services for the support of integrated security systems and solutions • Interfacing with the client in the strategic design process to translate security and business requirements into technical designs • Assisting with configuration, validating secure complex systems, and testing security products and systems to detect security weaknesses	
Cyber Security Engineer 3	Participates in special projects or investigations into specific technology or solution issues and research and piloting of new technologies. Serves as a point of contact for engineering efforts while maintaining compliance with the customer's policies and guidelines. Duties may include: • Configuring and maintaining policies • Maintaining documentation for exceptions to standards • Providing timely and adequate response to threats/alerts • Assessing security events to drive to a resolution • Providing timely and sufficient response to security incidents and assessment services • Promoting security awareness	Bachelor's degree, 6 years' experience
Cyber Security Engineer 4	Participates in special projects or investigations into specific technology or solution issues and research and piloting of new technologies. Serves as a point of contact for engineering efforts and maintains compliance with the customer's policies and guidelines. Duties may include: • Leading team of security engineers, managing large-scale deployment, assessment, and O&M projects • Validating and verifyig system security requirements definitions and analyses and establishes system security designs • Designing, developing, implementing and/or integrating IA and security systems and system components, including those for networking, computing, and enclave environments • Building IA into systems deployed to operational environments	Bachelor's degree, 8 years' experience
Cyber Subject-Matter Authority (SMA) 1	Recognized as an authority in a given domain of cyber security, or proficient in highly demanded emergent cyber tools or processes required under special circumstances. Duties may include applying subject-matter authority to a specific incident, security application, or enterprise environment to improve security posture or resolve organizational issues.	Bachelor's degree, 12 years' experience
Cyber Subject Matter Authority (SMA) 2	Recognized as an authority in a given domain of cyber security, or proficient in highly demanded emergent cyber tools or processes required under special circumstances. Duties may include: • Applying subject-matter authority to a specific incident, security application, or enterprise environment to improve security posture or resolve organizational issues • Generating issue papers and reporting	Bachelor's degree, 14 years' experience
Cyber Subject Matter Authority (SMA) 3	Recognized as an authority in a given domain of Cyber security, or proficient in highly demanded emergent cyber tools or processes required under special circumstances. Duties may include: • Applying subject-matter authority to a specific incident, security application, or enterprise environment to improve security posture or resolve organizational issues • Generating issue papers and reporting • Advising senior leadership on security issues	Bachelor's degree, 16 years' experience

Job Titles	Functional Responsibilities	Minimum Education and Experience
Cyber Senior Program Manager	Has overall accountability for Cyber programs. May be responsible for product delivery and financial management of client engagements. Performs independent quality assurance reviews of program performance and deliverables to ensure that contractual obligations are being met. Recognized expert in the areas of cyber process and the protection of technical architecture. Lends thought leadership to engagement teams in developing creative solutions to client problems.	Bachelor's degree, 15 years' experience
Cyber Project Manager	Manages, plans, and coordinates activities of cyber projects. Reviews project proposal or plan to determine schedule, funding limitations, procedures for accomplishing projects, staffing requirements, and allotment of available resources to various phases of projects. Establishes work plans and coordinates staffing for each phase of projects and arranges for recruitment or assignment of project personnel. Identifies functional and cross-functional requirements and resources required for each task.	Bachelor's degree, 10 years' experience
Cyber Task Manager	Applies broad management skills and specialized functional and technical expertise to guide cyber engineering and process teams in delivering client solutions or to manage the day-to-day operations of cyber projects. Monitors quality across multiple projects. Establishes and maintains financial and technical reports to show progress of projects to management and customers, organizes and assigns responsibilities to subordinates, and oversees the assigned tasks.	Bachelor's degree, 7 years' experience
Cyber Technical Architect 1	Provides thought leadership related to current and future customer plans with regard to protecting customer information technology from cyber threats. Possesses knowledge of the future direction and trends associated with the stated information technology, and is up to date with current threats associated with it. Experienced in designing and implementing protections for information architecture solutions for the stated information technology. Designs secure architecture to include the software, hardware, and communications to support the total requirements as well as provide for present and future cross-functional requirements and interfaces.	Bachelor's degree, 7 years' experience
Cyber Technical Architect 2	Provides thought leadership related to current and future customer plans with regard to protecting customer information technology from cyber threats. Possesses knowledge of the future direction and trends associated with the stated information technology, and is up to date with current threats associated with it. Experienced in designing and implementing protections for information architecture. Designs secure architecture to include the software, hardware, and communications to support the total requirements as well as provide for present and future cross-functional requirements and interfaces.	Bachelor's degree, 10 years' experience
Cyber System Administrator 2	May develop, run tests on, implement, and maintain operating system and related software in support of cyber related activities. Establishes and implements standards for computer operations, consistent with documented customer cyber policies, for compatibility between hardware and software, according to specifications and parameters. Troubleshoots and resolves software, operating system, and networking problems identified in vulnerability scans, penetration tests, and other security testing performed on the system. Schedules, performs, and monitors system backups and, when necessary, performs data recoveries.	Bachelor's degree, 3 years' experience

Job Titles	Functional Responsibilities	Minimum Education and Experience
Cyber System Administrator 3	Administers, develops, runs tests on, implements, and maintains operating system and related software in support of cyber related activities. Establishes and implements standards for computer operations, consistent with documented customer cyber policies, for compatibility between hardware and software, according to specifications and parameters. Troubleshoots and resolves software, operating system, and networking problems identified in vulnerability scans, penetration tests, and other security testing performed on the system. Schedules, performs, and monitors system backups and, when necessary, performs data recoveries. Competent in cyber subject matter and concepts and generally considered a specialist in area of assignment. May lead individuals assisting in the work.	Bachelor's degree, 7 years' experience
Cyber Database Administrator 2	Administers organization's database, using database management system to organize and store data. Ascertains user requirements, creates computer databases, and tests and coordinates changes. Interacts with cyber, development, and end-user personnel to determine application data access requirements, transaction rates, volume analysis, and other pertinent data required to develop and maintain integrated databases consistent with customer cyber policies. Ensures performance of database, including maintenance of proper accesses, and responds to issues that arise during security tests. May deploy and test security patches as released by commercial software vendors.	Bachelor's degree, 3 years' experience
Cyber Database Administrator 3	Administers organization's database, using database management system to organize and store data. Ascertains user requirements, creates computer databases, and tests and coordinates changes. Interacts with cyber, development, and end-user personnel to determine application data access requirements, transaction rates, volume analysis, and other pertinent data required to develop and maintain integrated databases consistent with customer cyber policies. Ensures performance of database, including proper maintenance of proper accesses, and responds to issues that arise during security tests, May deploy and test security patches as released by commercial software vendors.	Bachelor's degree, 7 years' experience
Cyber Functional Specialist 3	May provide knowledge in cyber industry, process, or technology areas. Duties may include: • Planning and managing the work of cyber information systems project teams • Designing and implementing new organizational structures • Assisting an organization in translating its vision and strategy into core human resource and cyber processes • Leading clients through streamlining, reengineering, and transforming processes to be more cyber centric • Developing and executing project budgets	Bachelor's degree, 8 years' experience
Cyber Programmer 1	Responsible for activities such as program design, coding, testing, debugging, and documentation. Has technical knowledge of and responsibility for cyber tools used in part or all of the cyber protection program employed in support of applications systems analysis and programming; understands the business or function for which application is designed. Duties may include: • Writing programs according to specifications, which may be provided by engineers, technical architects, or other computer scientists	Bachelor's degree

Job Titles	Functional Responsibilities	Minimum Education and Experience
	• Updating, repairing, modifying, and expanding existing computer programs	
Cyber Programmer 2	Responsible for activities such as program design, coding, testing, debugging, and documentation. Has technical knowledge of and responsibility for cyber tools used in part or all of the cyber protection program employed in support of applications systems analysis and programming; understands the business or function for which application is designed. Duties may include: • Writing programs according to specifications, which may be provided by engineers, technical architects, or other computer scientists • Updating, repairing, modifying, and expanding existing computer programs	Bachelor's degree, 2 years' experience
Cyber Programmer 3	Responsible for activities such as program design, coding, testing, debugging, and documentation. Has technical knowledge of and responsibility for cyber tools used in part or all of the cyber protection program employed in support of applications systems analysis and programming; understands the business or function for which application is designed. Duties may include: • Writing programs according to specifications, which may be provided by engineers, technical architects, or other computer scientists • Updating, repairing, modifying, and expanding existing computer programs	Bachelor's degree, 5 years' experience
Cyber Operations Manager	Mmanages, coordinates, or organizes department cyber operation strategies and activities. Duties may include: • Collaborating in the development and implementation of organization cyber policies, practices, procedures, and attainment of operating goals • Reviewing, analyzing, and preparing reports, records, and directives, and conferring with managers/supervisors to obtain data required for planning activities, such as new commitments, status of work in progress, and problems encountered • Disseminating policies and objectives to supervisors/staff	Bachelor's degree, 3 years' experience
Cyber Data Architect	May define, design, or develop relational and/or multi-dimensional databases for warehousing of data. Reviews current data structures and recommends optimizations and reconfigurations as warranted.	Bachelor's degree, 7 years' experience
Cyber Program Analyst	Analyzes and critiques existing computer programs and systems security measures, and develops new measures. Duties may include: • Reviewing users' requests for new or modified computer programs to determine feasibility, cost and time required, compatibility with current system, and security capabilities • Outlining steps required to develop program, using structured security analysis and design • Planning, developing, testing, and documenting computer programs, applying knowledge of cyber security, programming techniques, and computer systems	Bachelor's degree, 2 years' experience
Cyber Application Architect	May plan, design, develop, redesign or enhance, install, or implement various cyber technology products, or enhance computer programs. Applies knowledge of software and programming to develop and test the security of computer systems and produce the necessary outcome	Bachelor's degree, 3 years' experience

Job Titles	Functional Responsibilities	Minimum Education and Experience
	for clients. May draft technical white papers to help users better understand the cyber technology and to provide instructions that help the client better understand the nature and applications of a specific cyber product.	
Cyber Application Systems Analyst	The Cyber Application System Analyst may Oversee the implementation of required hardware and software security components for approved applications, coordinates security tests of the application system to ensure proper performance, and develops diagrams and flow charts for computer programmers to follow. This individual previews, analyzes, and modifies programming systems, including encoding, debugging, and installing security measures to support an organization's application systems. Develops application specifications, identifies the required inputs, and formats the output to meet users' needs.	Bachelor's degree, 4 years' experience
Cyber Security Specialist 1	May identify and resolve highly complex issues to prevent cyber attacks on information systems and to keep computer information systems secure from interruption of service, intellectual property theft, network viruses, data mining, financial theft, and theft of sensitive customer data, allowing business to continue as normal. This is accomplished through the systematic implementation of a cyber framework and process. Designs, installs, and manages security mechanisms that protect networks and information systems against hackers, breaches, viruses, and spyware. Responds to incidents, investigates violations, and recommends enhancements to plug potential security gaps. Performs more routine aspects of the position and is supervised by higher levels.	Bachelors' degree
Cyber Security Specialist 2	May identify and resolve highly complex issues to prevent cyber attacks on information systems and to keep computer information systems secure from interruption of service, intellectual property theft, network viruses, data mining, financial theft, and theft of sensitive customer data, allowing business to continue as normal. This is accomplished through the systematic implementation of a cyber framework and process. Designs, installs, and manages security mechanisms that protect networks and information systems against hackers, breaches, viruses, and spyware. Responds to incidents, investigates violations, and recommends enhancements to plug potential security gaps. Performs more varied and difficult tasks compared to Level 1, yet has less autonomy than Level 3.	Bachelor's degree, 3 years' experience
Cyber Security Specialist 3	May identify and resolve highly complex issues to prevent cyber attacks on information systems and to keep computer information systems secure from interruption of service, intellectual property theft, network viruses, data mining, financial theft, and theft of sensitive customer data, allowing business to continue as normal. This is accomplished through the systematic implementation of a cyber framework and process. Designs, installs, and manages security mechanisms that protect networks and information systems against hackers, breaches, viruses, and spyware. Responds to incidents, investigates violations, and recommends enhancements to plug potential security gaps. Is competent in subject matter and concepts and generally considered a specialist in area of assignment. May lead individuals assisting in the work.	Bachelor's degree, 7 years' experience
Cyber Network Administrator	Administers design, organization, and implementation of network, and heads technical support staff who manage and maintain hubs, servers,	Bachelor's degree,

Job Titles	Functional Responsibilities	Minimum Education and Experience
	firewalls, and routers. Uses knowledge and understanding of both networking and telecommunications theory and practice to protect system assets. Communicates with users, technical teams, and vendors on new technology and system upgrades and to determine software and hardware installation requirements.	3 years' experience
Cyber Enterprise Architect	Works with stakeholders, both leadership and subject-matter experts, to build a holistic view of the organization's strategy, processes, information, and IT assets to ensure that the business and IT are in alignment and protected from cyber threats. Links the business mission, strategy, and processes of an organization to its IT strategy, including security, and documents this using multiple architectural models or views that show how the current and future needs of an organization will be met in an efficient, sustainable, agile, secure, and adaptable manner.	Bachelor's degree, 8 years' experience
Cyber Training Specialist	Develops teaching outlines and determines instructional methods, using knowledge of specified training needs and effectiveness of such methods as individual training, group instruction, lectures, demonstrations, conferences, meetings, or workshops. Prepares, organizes, and heads training sessions covering standard training, specialized training, or counseling in designated areas.	Bachelor's degree, 2 years' experience
Cyber Storage Administrator	Administers and safeguards efficient and reliable centralized electronic storage area networks (SAN), such as Network Attached Storage, Content Addressable Storage, DAS environments, or other technologies classified as storage technology. May oversee, evaluate, implement, monitor, troubleshoot, or maintain SAN and related technologies, system upgrades, or optimization storage strategies. Monitors the data storage needs of the company so that business can run efficiently.	Bachelor's degree, 3 years' experience

Education and Experience Equivalents / Substitution Guide	
General equivalency guidelines for education, certifications, and experience are provided below.	
Required Experience or Degree or Relevant Certification	**Equivalent Experience or Degree**
1 year specialized experience	3 years' general professional experience
Relevant certification (e.g., CISSP, PMP, CCNA, etc.)	3 months' specialized experience
Associate's degree in Computer Science, Information Systems, Engineering, Business, or a scientific or technical discipline related to the specific skill	1.5 years' specialized experience
Bachelor's degree in Computer Science, Information Systems, Engineering, Business, or a scientific or technical discipline related to the specific skill	3 years' specialized experience
Master's degree in Computer Science, Information Systems, Engineering, Business, or a scientific or technical discipline related to the specific skill	5 years' specialized experience
Doctorate in Computer Science, Information Systems, Engineering, Business, or a scientific or technical discipline related to the specific skill	7 years' specialized experience

3. APPROVED GSA SCHEDULE PRICELIST

Labor Category	Price Offered to GSA (including IFF)
Program Manager 6	$184.13
Program Manager 5	$175.62
Program Manager 4	$146.35
Program Manager 3	$120.91
Telecommunications SME/Scientist 6	$232.14
Telecommunications SME/Scientist 5	$194.66
Telecommunications SME/Scientist 4	$180.76
Telecommunications SME/Scientist 3	$162.22
Network Engineer 5	$183.78
Network Engineer 4	$174.11
Network Engineer 3	$146.60
Network Engineer 2	$124.43
Network Engineer 1	$114.86
Network Solutions Architect 5	$175.92
Network Solutions Architect 4	$166.15
Network Solutions Architect 3	$153.15
Network Solutions Architect 2	$125.74
Network Solutions Architect 1	$106.40
Systems Architect 5	$178.94
Systems Architect 4	$158.69
Systems Architect 3	$135.57
Systems Architect 2	$109.32
Systems Architect 1	$85.64
Systems Engineer 5	$155.06
Systems Engineer 4	$154.16
Systems Engineer 3	$134.51
Systems Engineer 2	$111.34
Systems Engineer 1	$84.63
Systems Integrator 5	$153.40
Systems Integrator 4	$143.58
Systems Integrator 3	$123.78
Systems Integrator 2	$100.86
Systems Integrator 1	$75.37
BPI / Ops Research SME 5	$165.74
BPI / Ops Research SME 4	$154.61
BPI / Ops Research SME 3	$120.50
Vulnerability Assessment Analyst and Penetration Tester 1	$105.75
Vulnerability Assessment Analyst and Penetration Tester 2	$136.95
Vulnerability Assessment Analyst and Penetration Tester 3	$186.04
Vulnerability Assessment Analyst and Penetration Tester 4	$213.74
Incident Response Analyst 1	$91.04
Incident Response Analyst 2	$118.74
Incident Response Analyst 3	$162.28
Incident Response Analyst 4	$186.04
Security Operations Center (SOC) Analyst 1	$59.38
Security Operations Center (SOC) Analyst 2	$80.74
Security Operations Center (SOC) Analyst 3	$91.04
Security Operations Center (SOC) Analyst 4	$140.91

Labor Category	Price Offered to GSA (including IFF)
Cyber Hunter 1	$105.75
Cyber Hunter 2	$158.31
Cyber Hunter 3	$213.74
Cyber Hunter 4	$307.14
Risk and Vulnerability Threat Analyst 1	$91.04
Risk and Vulnerability Threat Analyst 2	$125.06
Risk and Vulnerability Threat Analyst 3	$162.28
Risk and Vulnerability Threat Analyst 4	$218.49
Cyber Security Engineer 1	$105.75
Cyber Security Engineer 2	$158.31
Cyber Security Engineer 3	$213.74
Cyber Security Engineer 4	$282.59
Cyber Subject-Matter Authority (SMA) 1	$376.81
Cyber Subject Matter Authority (SMA) 2	$419.56
Cyber Subject Matter Authority (SMA) 3	$490.80
Cyber Senior Program Manager	$428.27
Cyber Project Manager	$240.65
Cyber Task Manager	$186.04
Cyber Technical Architect 1	$186.04
Cyber Technical Architect 2	$240.65
Cyber System Administrator 2	$158.31
Cyber System Administrator 3	$186.04
Cyber Database Administrator 2	$136.95
Cyber Database Administrator 3	$162.28
Cyber Functional Specialist 3	$193.16
Cyber Programmer 1	$83.11
Cyber Programmer 2	$132.20
Cyber Programmer 3	$178.11
Cyber Operations Manager	$143.28
Cyber Data Architect	$185.23
Cyber Program Analyst	$105.75
Cyber Application Architect	$128.24
Cyber Application Systems Analyst	$160.71
Cyber Security Specialist 1	$105.75
Cyber Security Specialist 2	$136.95
Cyber Security Specialist 3	$185.23
Cyber Network Administrator	$143.28
Cyber Enterprise Architect	$218.04
Cyber Training Specialist	$143.28
Cyber Storage Administrator	$136.95