Federal Supply Service
Authorized Federal Supply Schedule Price List

U.S. General Services Administration

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

General Purpose Commercial Information Technology Equipment, Software and Services

SIN	DESCRIPTION	FSC CLASS/FPDS CODE
132-51	IT Professional Services	D302, D306, D308 & D311
132-45B	Incident Response	D399
132-45C	Cyber Hunt	D399
132-45D	Risk and Vulnerability	D399

Horizon Industries, Limited
8245 Boone Blvd. Ste. 300
Vienna, VA 22182
(TEL) 703.955.4665 (FAX) 703.242.2325
www.hil.us

Contract No.: 47QTCA19D0032
Period Covered by Contract: December 10th, 2018 – December 9th, 2023

Business Classification: Minority Owned Small Business

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

TABLE OF CONTENTS

CUSTOMER INFORMATION:

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

1b.

Lowest Priced Labor Category	Price
Technical Writer	$51.69/hr.

1c. Description of IT Services

2. Maximum order: *$500,000*

3. Minimum order: *$100.00*

4. Geographic coverage: *Domestic Delivery Only*

5. Point(s) of production: *Vienna, Fairfax County, Virginia*

6. Discount from list prices or statement of net price: *Prices shown are net, discounts have been applied.*

6. **Quantity Discounts.** *None*

7. Prompt payment terms. *Net 30 days from receipt of invoice or date of acceptance, whichever is later.*

9a &b Notification that Government purchase cards are accepted at or below the micro-purchase threshold. *Horizon Industries accepts credit card payment below and above the micro purchase threshold.*

10. Foreign items (list items by country of origin). *N/A*

11a. Time of delivery. *Horizon Industries shall deliver to destination within the number of calendar days specified on the order and as negotiated between the ordering activity and Horizon Industries.*

11b. Expedited Delivery. *If Horizon resources are available, Horizon Industries shall deliver services as soon as possible.*

11c. Overnight and 2-day delivery. *If Horizon resources are available, the customer may contact Horizon for rates for overnight and 2-day delivery.*

11d. Urgent Requirements. *Agencies may contact Horizon for any urgent requirement.*

12. F.O.B. point. *Destination*

13a. Ordering address: *Horizon Industries Limited, 8245 Boone Blvd., Suite 300, Vienna, VA 22182*

13b. Ordering procedures: *For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPA's) are found in Federal Acquisition Regulation (FAR) 8.405-3.*

14. Payment address(es): *Horizon Industries Limited, 8245 Boone Blvd., Suite 300, Vienna, VA 22182*

15. Warranty provision. *N/A*

16. Export packing charges, if applicable. *N/A*

17. **Terms and conditions of Government purchase card acceptance (any thresholds above the micro-purchase level).** *N/A*

18. Terms and conditions of rental, maintenance, and repair (if applicable). *N/A*

19. Terms and conditions of installation (if applicable). *N/A*

20. Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices (if applicable). *N/A*

20a. Terms and conditions for any other services (if applicable). *N/A*

21. List of service and distribution points (if applicable). *N/A*

22. List of participating dealers (if applicable). *N/A*

23. Preventive maintenance (if applicable). *N/A*

24a. Special attributes such as environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants). *N/A*

24b. If applicable, indicate that Section 508 compliance information is available on Electronic and Information Technology (EIT) supplies and services and show where full details can be found (e.g. contractor's website or other location.) The EIT standards can be found at: www.Section508.gov/.

25. Data Universal Number System (DUNS) number: *965557507*

26. Notification regarding registration in Central Contractor Registration (CCR) database. Horizon Industries is registered in the System for Award Management (SAM).
CAGE Code: 1UH05

TERMS AND CONDITIONS APPLICABLE TO HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS) (SPECIAL ITEM NUMBERS 132-45A, 132-45B, 132-45C and 132-45D)

Vendor suitability for offering services through the Highly Adaptive Cybersecurity Services (HACS) SINs must be in accordance with the following laws and standards when applicable to the specific task orders, including but not limited to:

● Federal Acquisition Regulation (FAR) Part 52.204-21
● OMB Memorandum M-06-19 - Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments
● OMB Memorandum M -07-16 - Safeguarding Against and Responding to the Breach of Personally Identifiable Information
● OMB Memorandum M-16-03 - Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements
● OMB Memorandum M-16-04 – Cybersecurity Implementation Plan (CSIP) for Federal Civilian Government
● The Cybersecurity National Action Plan (CNAP)
● NIST SP 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
● NIST SP 800-27A - Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
● NIST SP 800-30 - Guide for Conducting Risk Assessments
● NIST SP 800-35 - Guide to Information Technology Security Services
● NIST SP 800-37 - Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
● NIST SP 800-39 - Managing Information Security Risk: Organization, Mission, and Information System View
● NIST SP 800-44 - Guidelines on Securing Public Web Servers
● NIST SP 800-48 - Guide to Securing Legacy IEEE 802.11 Wireless Networks
● NIST SP 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations
● NIST SP 800-61 - Computer Security Incident Handling Guide
● NIST SP 800-64 - Security Considerations in the System Development Life Cycle
● NIST SP 800-82 - Guide to Industrial Control Systems (ICS) Security
● NIST SP 800-86 - Guide to Integrating Forensic Techniques into Incident Response
● NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment
● NIST SP 800-128 - Guide for Security-Focused Configuration Management of Information Systems
● NIST SP 800-137 - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
● NIST SP 800-153 - Guidelines for Securing Wireless Local Area Networks (WLANs)
● NIST SP 800-171 - Protecting Controlled Unclassified Information in non-federal Information Systems and Organizations

1. SCOPE

a. The labor categories, prices, terms and conditions stated under Special Item Numbers 132-45A, 132-45B, 132-45C and 132-45D High Adaptive Cybersecurity Services apply exclusively to High Adaptive Cybersecurity Services within the scope of this Information Technology Schedule.

b. Services under these SINs are limited to Highly Adaptive Cybersecurity Services only. Software and hardware products are under different Special Item Numbers on IT Schedule 70 (e.g. 132-32, 132-33, 132-8), and may be quoted along with services to provide a total solution.

c. These SINs provide ordering activities with access to Highly Adaptive Cybersecurity services only.

d. Highly Adaptive Cybersecurity Services provided under these SINs shall comply with all Cybersecurity certifications and industry standards as applicable pertaining to the type of services as specified by ordering agency.

e. 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. ORDER

a. Agencies may use written orders, Electronic Data Interchange (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.

3. PERFORMANCE OF SERVICES

a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity. All Contracts will be fully funded.

b. The Contractor agrees to render services 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 Highly Adaptive Cybersecurity 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. All travel will be agreed upon with the client prior to the Contractor's travel.

4. INSPECTION OF SERVICES

Inspection of services is in accordance with 552.212-4 - CONTRACT TERMS AND CONDITIONS – COMMERCIAL ITEMS (MAY 2015) (ALTERNATE II – JUL 2009) (FAR DEVIATION – JUL 2015) (TAILORED) for Firm-Fixed Price and Time-and-Materials and Labor-Hour Contracts orders placed under this contract.

5. 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 (MAY 2014) Rights in Data – General, may apply.

The Contractor shall comply with contract clause (52.204-21) to the Federal Acquisition Regulation (FAR) for the basic safeguarding of contractor information systems that process, store, or transmit Federal data received by the contract in performance of the contract. This includes contract documents and all information generated in the performance of the contract.

6. RESPONSIBILITIES OF THE ORDERING ACTIVITY

Subject to the ordering activity's security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite Highly Adaptive Cybersecurity Services.

7. INDEPENDENT CONTRACTOR

All Highly Adaptive Cybersecurity 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.

8. 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.

9. INVOICES
The Contractor, upon completion of the work ordered, shall submit invoices for Highly Adaptive Cybersecurity 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.

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

11. 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.

12. DESCRIPTION OF HIGHLY ADAPTIVE CYBERSECURITY SERVICES AND PRICING
a. The Contractor shall provide a description of each type of Highly Adaptive Cybersecurity Service offered under Special Item Numbers 132-45A, 132-45B, 132-45C and 132-45D for Highly Adaptive Cybersecurity Services and it should be presented in the same manner as the Contractor sells to its commercial and other ordering activity customers. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles (labor categories) for those individuals who will perform the service should be provided.

b. Pricing for all Highly Adaptive Cybersecurity Services shall be in accordance with the Contractor's customary commercial practices; e.g., hourly rates, minimum general experience and minimum education.

TERMS AND CONDITIONS APPLICABLE TO INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES (SIN 132-51)

NOTE: *All non-professional labor categories must be incidental to, and used solely to support professional services, and cannot be purchased separately.*

1. SCOPE

a. The prices, terms and conditions stated under Special Item Number 132-51 Information Technology Professional Services apply exclusively to IT Professional Services within the scope of this Information Technology 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 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 Blanket Purchase Agreements under this contract.

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

In accordance with FAR 52.212-4 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 (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, 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 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. 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 PROFESSIONAL SERVICES AND PRICING
a. The Contractor shall provide a description of each type of IT Service offered under Special Item Numbers 132-51 IT Professional Services should be presented in the same manner as the Contractor sells to its commercial and other ordering activity customers. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles (labor categories) for those individuals who will perform the service should be provided.

b. Pricing for all IT Professional Services shall be in accordance with the Contractor's customary commercial practices; e.g., hourly rates, monthly rates, term rates, and/or fixed prices, minimum general experience and minimum education.

Labor Category Descriptions

Program Manager

Functional Responsibility: Works to assist customer's key management and lead personnel to realize maximum benefit from an investment in IT equipment, personnel and business processes. Provides expert guidance in analysis, strategic planning, quality management, change management, business process re-engineering and the design of information technology architectures. Conducts needs analysis, functional, technical and logical analysis, feasibility studies, cost-benefit studies, life cycle analysis, briefings and presentations, report writing and post-implementation projects. Manages multidisciplinary projects from inception to final deliverable, involving lead computer engineers, systems analysts and computer programmers, business analysts to achieve an integrated IT solution to customer's requirements. Organizes, directs, and coordinates planning and execution of all program/technical support activities. Simultaneously plans and manages transition of several highly technical projects. Establishes or alters (as necessary) management structure to effectively direct program/technical support activities. Meets and confers with client management regarding the status of specific program/technical activities as well as problems, issues, or conflicts requiring resolution.

Minimum/General Experience: Possesses thorough knowledge of IT processes, principles and practices involved in computer-aided technical solutions. Must have an understanding of systems analysis, cost analysis and processes relevant to planned assignments. Has a minimum of three years working experience in a technical management capacity. Has demonstrated information technology expertise and communication skills to be able to interface with all levels of management.

Minimum Education: Master's Degree in Computer Science or Equivalent Experience.

Systems Analyst

Functional Responsibility: Analyzes information system processing and design requirements across a range of capabilities, including numerous engineering, technical, business, and records management functions. Develops plans for information systems from project inception to conclusion. Analyzes system problems, support requirements, and the information to be processed. Conducts needs analysis, functional, technical and logical analysis, feasibility studies, cost-benefit studies, life cycle analysis, briefings and presentations, report writing and post- implementation projects. Defines the problem/support needed, and develops system requirements and program specifications, from which programmers prepare detailed flow charts, programs, and tests. Coordinates closely with programmers, business process owners and software engineers to ensure implementation of program and systems specifications. Develops business process charts, performs financial modeling, and assist with change management. Provides evaluation on a technical, functional, or cost basis for system design, development, and/or maintenance. Assists with and/or performs database design and development.

Minimum/General Experience: Minimum of 2 years technical experience. Possesses vast experience in evaluating, developing and/or analyzing information systems (IS) or information technology (IT), financial analysis and business process modeling. This experience includes the use of client-server systems, distributed databases, both wide-area and local-area communications, and a performance-based acquisition process. A person in this category is expected to have knowledge of quality assurance standards, testing strategies, and certification compliance.

Minimum Education: Bachelor's Degree Computer Science, Computer Information Systems, Business, Mathematics, or Equivalent Technical Studies/experience.

Program Specialist

Functional Responsibility: Participates in the analysis of functional business/technical applications and design specifications for functional activities. Performs detailed financial and economic modeling. Interacts with functional and technical personnel to translate detailed design into computer application software. Provides unique and/or in-depth technical or business analysis and technical/business report development support within subject-matter areas requiring leading-edge or state-of-the-art technical and business expertise. May support a wide variety of technical and business assignments based on the specific needs of the task's requirements. Analyzes information system user needs to determine functional requirements. Performs functional allocation to identify required tasks and their interrelationships. Identifies resources and costs required for each information system development and/or maintenance task. Evaluates systems and business processes to conduct Fit- Gap or other related analysis. Prepares plans for COTS implementations including transition plans and staffing requirements.

Minimum/General Experience: Minimum of 1 year technical experience. IT/Financial specialist with working experience in finance, business analysis, systems functional analysis, quality management, database development, or data administration/standardization. Acquired skills include computer modeling and simulation. Trained in technical, cost, or business discipline specific to assignment. Working knowledge and/or familiarity with systems acquisition and RFP process.

Minimum Education: Bachelor's Degree in Computer Science, Information Systems, Engineering, Business, or other related discipline, or Equivalent Experience in a technical or business discipline.

Documentation Specialist

Functional Responsibility: Participates in the performance of needs analysis, functional, technical and logical analysis, feasibility studies, cost-benefit studies, life cycle analysis, briefings and presentations, report writing and post-implementation projects. Assists with all stages of source selection and the proposal process including the preparation of Requests for Information (RFI), Requests for Proposals (RFP) and Requests for Quotations (RFQ). Manages the data collection process and the development and maintenance of databases to support program/project management, data compilation, and the creation of final deliverables.

Minimum/General Experience: Ability to apply the disciplines of operations research to the analysis of problems. Acquired skills include computer modeling and simulation, data collection and statistical analysis, evaluation of strategies and tactics under risk scenarios, test planning and conduct, etc. Possesses skills utilizing software for the preparation of documents, spreadsheets, flow charts/diagrams, database structures, and presentations. Has strong organizational skills, experience utilizing project management software and knowledge of the Federal Acquisition process.

Minimum Education: Bachelor's Degree or Equivalent Experience

Technical Writer

Minimum/General Experience: Requires a minimum of 2 years' experience in technical research and writing. Must possess skills utilizing software for the preparation of documents, spreadsheets, flow charts/diagrams, database structures, and presentations. Has proven organizational skills, experience utilizing project management software and knowledge of the Federal Acquisition process.

Functional Responsibility: Gathers, analyzes, and composes technical and financial information required for project engagements. Assist with/creates presentations, user manuals, help documentation, training materials, and installation guides. Assists with the development of technology related procurements. Provides assistance in preparing proposals, Requests for Information (RFI), Requests for Proposals (RFP) and Requests for Quotations (RFQ), presentations, reports and other client deliverables/documents as appropriate.

Minimum Education: Associate Degree or Equivalent Experience

Senior IT Analyst/Designer

Functional Responsibility: Perform business and technical analyst functions, including workshop facilitation, business process data validation, application testing from a functional business area perspective, program development, unit testing of the application code from a technical perspective, work group/work session participation, and delivery of technical and business solutions. Implements data bases that are the result of business system planning and data requirement planning. Provides for systems development and data base administration groups the future business strategies as seen from a data point of view. Assists with the analysis of information system baseline and perform a "gap analysis" between the baseline, the user operational requirements and the operating capability of enterprise application product sets. Also perform business and technical designer functions, including making contribution to both the business and technical architecture components of the solution, supporting industry/functional area/business process specialists and experts, supporting architecture/product/technology specialists and experts, and review/assess enterprise solution products for accuracy and consistency. Provides work direction and guidance to other personnel; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks.

Minimum/General Experience: Requires seven years of application team experience. May team lead or serve as a project manager, including planning tasks, assigning resources to the task, monitoring and tracking progress, and informing project management on all project activities. Possess a thorough knowledge of IT processes, principles and practices involved in technical solutions. Has an understanding of systems analysis, cost analysis and processes relevant to planned assignments. Has demonstrated information technology expertise and communication skills to be able to interface with all levels of management.

Minimum Education: Master's Degree in Computer Science, Computer Information Systems, Business, Mathematics, or Equivalent Technical Studies/experience.

Project Manager

Functional Responsibility: Responsible for all aspects of assigned projects and provides a single point of contact for those projects. Manages the definition of project scope and objectives. Manages the development of detailed work plans, schedules, project estimates, resource plans including budgets, and status reports. Conducts project meetings and is responsible for project tracking and analysis. Ensures adherence to quality standards and reviews project deliverables. Manages the integration of subcontractor tasks and tracks and reviews subcontractor deliverables. Provides technical and analytical guidance to project team. Recommends and takes action to direct the analysis and solutions of problems.

Minimum/General Experience: Minimum of 7 years of experience is required, which includes all aspects of project management. Must be able to interact with all levels of client representatives. Must possess strong interpersonal skills and have strong writing abilities.

Minimum Education: Bachelor's Degree in Computer Science, Information Systems, Engineering, Business or Equivalent Experience.

Trainer/Facilitator

Functional Responsibility: Develops, directs, plans, delivers and evaluates training programs or IT facilitator activities. Provides direct instruction and training to customers on services, procedures, processes, techniques, tactics, products or skill development.

Minimum/General Experience: Minimum of 2 years relevant experience is required. Must possess strong interpersonal skills and have strong writing abilities.

Minimum Education: Bachelor's Degree in subject-related technical or business area, or Equivalent Experience.

Sr. Trainer/Facilitator
Functional Responsibility: Develops, directs, plans, delivers and evaluates training programs or IT facilitator activities. Provides direct instruction and training to customers on services, procedures, processes, techniques, tactics, products or skill development.
Minimum/General Experience: Minimum of 9 years relevant experience is required. Must possess strong interpersonal skills and have strong writing abilities.
Minimum Education: Bachelor's Degree in subject-related technical or business area, or Equivalent Experience.

Sr. Developer Consultant
Functional Responsibility: Serves as a senior member of consulting teams as a task manager or as a project leader on projects of limited scope and complexity. As a consulting team member, collects, analyzes, and interprets data in one or more information technology specialties. Develops, or participates in the development of IT solutions.
Minimum/General Experience: Minimum of 5 years of experience is required, which includes all aspects of project management. Must be able to interact with all levels of client representatives. Must possess strong interpersonal skills and have strong writing abilities.
Minimum Education: Bachelor's Degree in Computer Science, Information Systems, Engineering, Business or Equivalent Experience.

Systems Developer
Functional Responsibility: : Responsible for design development, coding, testing and debugging new IT solutions or significant enhancements to existing software. Works with technical staff to understand problems with IT solutions and develops specifications to resolve them. Resolves customer complaints and responds to suggestions for improvements and enhancements. Participates in the development of user manuals. May act as team leader on less complex projects. Assist in training less experienced software development staff.
Minimum/General Experience: Minimum of 3 years of experience is required. Must be able to participate as high-level technical expert.
Minimum Education: Bachelor's Degree in Computer Science, Information Systems, Engineering or Equivalent Experience.

Subject Matter Expert
Functional Responsibility: Provides unique and/or in-depth technical or business analyses and expertise within leading-edge or state-of-the-art technical and business areas. May support a wide variety of technical and business assignments based on the specific needs of the task's requirements.
Minimum/General Experience: Minimum of 5 years of experience is required providing technical expertise within a specific subject area or discipline. Must possess strong interpersonal skills and have strong writing abilities.
Minimum Education: Master's Degree in subject-related technical or business area, or Equivalent Experience.

Software Developer Consultant
Functional Responsibility: Serves as a consulting team member with a Software Development background. Collects data in accordance with plans developed by others. Verifies and analyzes data to identify trends and relationships as well as current and potential technical and management problems. Drafts reports of findings along with related documentation.
Minimum/General Experience: Minimum of 4 years of experience is required, which includes all aspects of project management. Must be able to interact with all levels of client representatives. Must possess strong interpersonal skills and have strong writing abilities.
Minimum Education: Bachelor's Degree in Computer Science, Information Systems, Engineering, Business or Equivalent Experience.

Sr. Program Specialist
Functional Responsibility: Participates in the analysis of functional business/technical applications and design specifications for functional activities. Performs detailed financial and economic modeling. Interacts with functional and technical personnel to translate detailed design into computer application software. Provides unique and/or in-depth technical or business analysis and technical/business report development support within subject-matter areas requiring technical and business expertise. May support a wide variety of technical and business assignments based on the specific needs of the task's requirements. Analyzes information system user needs to determine functional requirements. Performs functional allocation to identify required tasks and their interrelationships. Identifies resources and costs required for each information system development and/or maintenance task. Evaluates systems and business processes to conduct Fit-Gap or other related analysis. Prepares plans for implementations including transition plans and staffing requirements.
Minimum/General Experience: Minimum of 3 years of technical experience. IT/Financial specialist with working experience in finance, business analysis, systems functional analysis, quality management, database development, or data administration/standardization. Acquired skills include computer modeling and simulation. Trained in technical, cost, or business discipline specific to assignment. Working knowledge and/or familiarity with systems acquisition and RFP process.
Minimum Education: Bachelor's Degree in Computer Science, Information Systems, Engineering, Business, or other related discipline, or Equivalent Experience.

Program Analyst
Functional Responsibility: Assists and participates in developing program formulation and execution process by performing analyses and provide result for recommendations; identifies needs; monitors adjustment request to determine timely processing; compiles and prepares written reports on an ad hoc basis; reports require the ability to research, analyzes, interprets data, and sustains conclusions through the extensive use of supplemental computer applications to produce the final products; reviews various report, researches to correct invalid or erroneous transaction; maintain record management program.
Minimum/General Experience: Minimum 3 years of technical experience.
Minimum Education: Bachelor's Degree in Computer Science, Information Systems, Engineering, Business, or other related discipline, or Equivalent Experience.

Cyber Compliance Manager
Functional Responsibility: The Cyber Compliance Manager is accountable for the monitoring and enforcing compliance to IT and cyber security policies and governing procedures to reduce risk to cyber incidents and potential areas of non-compliance. Responsible for understanding and assessing technology and operational risks related to internal technology solutions and at times, might be asked to provide input to personnel on appropriate controls to address those risks.
Minimum/General Experience: Seven (7) years of relevant experience. Meets or exceeds current industry certification requirements. Experience with systems and network administration including Microsoft product environments (Windows Server, SharePoint Server, SQL Database, Project Server, Lync Server, and Exchange Server) specifically in the 2012 / 2013 versions, and Cisco environments to include perimeter routers, firewalls, IDS/IPS solutions, and network level 2/3 switch environment. Experience with cyber compliance methodologies.
Minimum Education: Bachelor's degree or equivalent.

Computer Network Defense (CND) Auditor
Functional Responsibility: Applies a technical and functional expertise to support network-based vulnerability scanning and computer network defense operations for large scale enterprise networks. Performs monthly and ad hoc vulnerability scans of unclassified and classified network subscriber enclaves. Maintain knowledge of emerging threats, vulnerabilities, and intelligence within the cyber security field to ensure subscribers are remediating against known threats. Assist subscribers with vulnerability remediation as necessary. Conduct trending and analysis of monthly results to identify high risk vulnerabilities impacting the network and ensure proper security posture from a vulnerability management standpoint. Deploy, troubleshoot, and maintain network-based vulnerability scanners at subscriber sites to ensure appropriate coverage of scanning services. Maintain knowledge of applicable CND policies, regulations, and compliance documents specifically related to CND auditing. Prepare reports for subscribers to assess technical configurations and compliance. Generate capture as necessary of the network(s) security posture and provide to CND management for situational awareness. Document policies and procedures for the use of vulnerability assessment tools and methodologies. Test and evaluate new technologies, specifically related to network vulnerability scanning.
Minimum/General Experience: Seven (7) years of relevant experience. Meets or exceeds current industry certification requirements. Understanding of Information Assurance (IA) and Computer Network Defense (CND) concepts, practices and tools to design and administer classified and unclassified DoD computer networks and systems. Ability to communicate complex technical and programmatic information, often in the form of verbal and visual operational updates, situation reports and briefings. Computer helpdesk, Systems Administration, Network Administration, and strong customer service skills preferred. Understanding of TCP/IP networking required, experience with cyber security related tools preferred. Familiarity of Windows Server/Workstation operating systems required, familiarity of Unix/Linux preferred. Familiarity with CJCSM 6510 and DoD 8570.1 (desired). Computer Emergency Response Team (CERT) or Security Operations Center (SOC) operations (desired).
Minimum Education: Bachelor's degree or equivalent.

Computer Security Systems Specialist
Functional Responsibility: Analyzes and defines security requirements for Multilevel Security (MLS) issues. Designs, develops, engineers and implements solutions to MLS requirements. Responsible for the implementation and development of the MLS. Gathers and organizes technical information about an organization's mission goals and needs, existing security products, and ongoing programs in the MLS arena. Performs risk analyses which also includes risk assessment. Provides technical support for secure software development and integration tasks, including reviewing work products for correctness and adhering to the design concept and to user standards. Knowledgeable of Security/Information Assurance (IA) products such as PKI, VPN, firewalls, and intrusion detection systems. Analyzes and recommends resolution of security/IA problems on the basis of knowledge of the major IA products and services, an understanding of their limitations, and knowledge of the IA disciplines.
Minimum/General Experience: Two (2) years of project related experience. Meets or exceeds current industry certification requirements.
Minimum Education: Bachelor's degree or equivalent.

Cyber Security Analyst
Functional Responsibility: Investigates and contributes to large scale, complex computer security incident response events on a global network. Leverages advanced tools to identify and mitigate malicious activity, ranging from malware to potential interactive intrusions. Analyzes computer systems and network traffic for signs of infection or compromise. Characterizes suspicious binaries and be able identify traits. Identify potential malicious activity from memory dumps, logs, and packet captures. Interact and assist other investigative teams on time sensitive, critical investigations. Participates as part of a close team of technical specialists on coordinated responses and subsequent remediation of security incidents. Serves as escalation point and performs further triage on escalated incidents and events. Provides briefings to leadership. Senior Cyber Security Analyst will act as a subject matter expert on information security related issues pertaining to malware analysis and incident response.
Minimum/General Experience: Two (2) years of project related experience. Meets or exceeds current industry certification requirements.
Minimum Education: Bachelor's degree or equivalent.

Cyber Security Operations Manager
Functional Responsibility: Leads Cyber Security Incident Response (CSIR) efforts across an organization including determination of the criticality of an incident, appropriate containment, and mitigation activities. Prioritizes advanced computer and network forensic investigations relating to various forms of malware, computer intrusion, theft of information, denial of service, and data breaches. Oversees the execution of Cyber Security Incident Response others for minor security incidents. Establishes and maintains strong working relationships with all teams required to support incident response. Improves Incident Response processes by taking advantage of and integration with new technologies and capabilities.
Minimum/General Experience: Five (5) years of project related experience. Meets or exceeds current industry certification requirements.
Minimum Education: Bachelor's degree or equivalent.

Cyber Security Program Manager
Functional Responsibility: Responsible for all contract activities for a Cyber Security related program. Sets policies and procedures, technical standards and methods, and priorities. Coordinates the management of all work performed on tasks under the contract. Coordinates the efforts of subcontractors, team members, and vendors. Acts as the central point of contact with the Contracting Officer, the Contracting Officer's Representative, and other client officials. Works independently, or under the general direction of senior level company management, on all phases of performance including contract management, project/task order management, coordination of resource needs, coordination with corporate resources and management.
Minimum/General Experience: Seven (7) years of project related experience. Meets or exceeds current industry certification requirements.
Minimum Education: Bachelor's degree or equivalent.

Cyber Security System Engineer
Functional Responsibility: Assist in planning, design, implementation, and maintenance of the enterprise computer network defense capabilities from the enterprise down to the end point. Assumes a key role in providing ongoing expertise for Client's tactical and strategic cyber Security incident response initiatives. Facilitates business enablement activities, including incident response, workflow & best practices and ensures key project milestones are achieved. Technical troubleshooting and root-cause analysis of solutions currently installed within the Client infrastructure. Assist with on-going architecture updates for diagrams, configuration guide(s), and supporting documentation when necessary. Leads the capture of relevant IT requirements and assists team leads and project managers with information assurance architecture and designs. Once deployed, maintains and tunes information assurance systems across network, data center, cloud, and at the application layer as needed. Integrates and customizes information assurance systems.
Minimum/General Experience: 4 years of project related experience. Strong command of networking and general IT, which can include OSI model, routing/switching and network security architecture, basic encryption, operating systems, Message transfer agents, Web Proxies, IDS. Meets or exceeds current industry certification requirements.
Minimum Education: Bachelor's degree or equivalent.

Cyber Threat Intelligence Analyst
Functional Responsibility: Provides cyber intelligence analysis including the reviews classified and unclassified cyber news feeds, signature updates, incident reports, threat briefs, and vulnerability alerts from external sources and to determine its applicability to the customer environment. Disseminates information externally within the cyber intelligence community. Interprets and compiles the information received about emerging threats at different classification levels through data feeds from Internet security firms, Government organizations, private industry, and foreign Governments into actionable monitoring either by developing custom content or by some other means. Identifies potential threats based on enterprise utilized hardware and software and accounts for current and evolving hacking tools and methodologies available to disrupt these systems. Participates in cybersecurity exercises. Designs, leads, or supports cybersecurity exercises and supports Blue Team/Red Team activity.
Minimum/General Experience: Two (2) years of project related experience. Meets or exceeds current industry certification requirements.
Minimum Education: Bachelor's degree or equivalent.

Ethical Hacker

Functional Responsibility: Performs application analysis, reverse engineering, malware analysis, protocol analysis, and debugging. Penetrates networks or computer systems to identify computer security vulnerabilities. Demonstrates a general understanding of how social engineering is used to compromise networks and end devices. Possesses proficient knowledge of multiple operating systems and hacking techniques. Possesses excellent communications skills and is comfortable speaking in public. Leads Red Teams and authors' penetration testing Rules of Engagement. Leads teams and oversees penetration testing. Working knowledge with commercial and open source tools and experience with multiple programming languages. Experience with hardware-based and software security exploits and experience with reverse engineering and assembly language. Experience supporting Red Teams in the Department of Defense, Homeland Security, Intelligence Community or other federal agencies.

Minimum/General Experience: Two (2) years of project related experience. Meets or exceeds current industry certification requirements.

Minimum Education: Bachelor's degree or equivalent.

Forensics Analyst

Functional Responsibility: Conducts forensic acquisition and analysis of cyber security incidents. Performs "Hunt Operations" actively searching for indicators of compromise. Provides information for the indicator database and assists with signature creation and tuning to ensure proper agency cyber defenses. Works directly with system administrators to remediate systems to mitigate and/or prevent incidents of compromise. Actively work to reduce and mitigate findings from "Hunt Operations" or from other assessments and will report progress as requested by the Government. Assists or leads digital forensics investigations. Experience maintaining chain of custody and cataloguing evidence/information related to forensics investigation. Experience in eDiscovery and possesses working knowledge of EnCase or similar forensics tools.

Minimum/General Experience: Three (3) years of project related experience. Meets or exceeds current industry certification requirements.

Minimum Education: Bachelor's degree or equivalent.

Incident Handler

Functional Responsibility: Performs and interprets vulnerability assessments and troubleshoots and resolves network/operating system security issues. Administers the operations of a security infrastructure and serves as a member of a security operations team monitoring all aspects of network security. Monitor, contextualize and provide reporting on a wide variety of network data feeds that may include network logs, syslogs, firewall logs, netflow data, and IDS/IPS logs. Leveraging experience in network exploitation and defense, maintain a current knowledge of attack vectors and methodologies and apply this knowledge to identify vulnerabilities in an assigned network. Serve as Incident Lead for response actions to security incidents including but not limited to External Cyber Attacks, Security Violations, Insider Threat Behaviors, Classified Spillages and Configuration-based Threats. Represent the Security Team in collaborative efforts across multiple Operations and Maintenance Teams to ensure risk awareness, security best-practices, and to assist these teams in deploying and maintaining the network at the lowest possible risk accepted by the client. Ensures system security needs established and maintained for operations development, security requirements definition, security risk assessment, systems analysis, systems design, security test and evaluation, certification and accreditation, systems hardening, vulnerability testing and scanning, incident response, disaster recovery, and business continuity planning and provides analytical support for security policy development and analysis. Integrates new architectural features into existing infrastructures, designs cyber security architectural artifacts, provides architectural analysis of cyber security features and relates existing system to future needs and trends, embeds advanced forensic tools and techniques for attack reconstruction, provides engineering recommendations, and

resolves integration and testing issues.
Minimum/General Experience: Two (2) years of project related experience. Possess one or more security related certifications, preferably GCIH or equivalent, CEH, etc. A solid foundation in networking, with a good understanding of TCP/IP and other core protocols. Experience in network, host, data and/or application security in a Windows/Unix/Linux operating environment. Background in information security operations e.g. incident response and monitoring services. Knowledge of network-based services and client/server applications. Experience with programming/scripting languages (e.g.Python/Perl). Experience with enterprise information security data management tools/SIEM such as ArcSight or Splunk.
Minimum Education: Bachelor's degree or equivalent.

Incident Responder
Functional Responsibility: Actively monitor systems and networks for intrusions. Identify security flaws and vulnerabilities. Perform security audits, risk analysis, network forensics and penetration testing. Perform malware analysis and reverse engineering. Develop a procedural set of responses to security problems. Establish protocols for communication within an organization during security incidents. Produce detailed incident reports and technical briefs for management, administrators and end-users. Liaison with other cyber threat analysis entities.
Minimum/General Experience: Two (2) years of project related experience. Possess one or more security related certifications, preferably GCIH or equivalent, CEH, etc. A solid foundation in networking, with a good understanding of TCP/IP and other core protocols. Experience in network, host, data and/or application security in a Windows/Unix/Linux operating environment. Background in information security operations e.g. incident response and monitoring services. Knowledge of network-based services and client/server applications. Experience with programming/scripting languages (e.g.Python/Perl). Experience with enterprise information security data management tools/SIEM such as ArcSight or Splunk.
Minimum Education: High School/GED

Incident Response Analyst
Functional Responsibility: Collects and analyzes cyber event information and performs threat or target analysis duties. Provides operations for persistent monitoring on a 24/7 basis of all designated networks, enclaves, and systems. Interprets, analyzes, and reports all events and anomalies in accordance with computer network directives, including initiating, responding, and reporting discovered events. Provides oversight of incident data flow and response, content, and remediation, and partners with other incident response centers in maintaining an understanding of threats, vulnerabilities, and exploits that could impact networks and assets. Performs real-time proactive security monitoring and reporting on various security enforcement systems, such as SIEM, anti-virus, internet content filtering/reporting, malcode prevention, firewalls, IDS & IPS, Web security, anti-spam, etc.
Minimum/General Experience: Two (2) years of related technical experience. Possess one or more security related certifications, preferably GCIH or equivalent, CEH, etc. Experience working cyber incident management, threat/network defense and troubleshooting.
Minimum Education: Bachelor's degree or equivalent.

Incident Response Coordinator
Functional Responsibility: Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Handle and response and forensic investigations in relation to computer security incidents and escalate when necessary as well as coordinate response to computer security incidents. Recommend a course of action on each incident and creates, manages, and records all actions taken and serve as initial POC for Events of Interest reported both internally and externally. Establishes alarm/incident escalation process and tracks, follows-up, and resolves incidents. Initiates and maintains contact with affected parties during incident response lifecycle. Investigates potential incidents/intrusions.
Minimum/General Experience: Three (3) years of project related experience. Possess one or more security related certifications
Minimum Education: Highschool/GED

Information Assurance Security Engineer
Functional Responsibility: Provide analysis of existing and emerging Information Systems and IT Infrastructure to assess compliance with applicable Information Assurance policy. Reviews both existing and draft/proposed policy against system design documentation and identify any areas of non-compliance. Assist with and/or conduct Security Test and Evaluation and IA assessment reviews as a way of validating compliance with IA policy. Review all proposed and draft policies and provide an assessment of the impact of the proposed policy on IT and IA architecture. Develop and document standards and guides for the implementation of IA solutions including but not limited to, compliance, system security design, security testing and IA assessments. Prepare training materials to assist in the transition of procedures and policies for the Cyber Security tools to client. Create baseline environments for hosting Cyber Security tools for intrusion detection/prevention systems (IDS/IPS), log aggregation/correlation, compliance monitoring and remediation, and Host Based Security System (HBSS) and other emerging technologies (hereafter referred to as Cyber Security tools).
Minimum/General Experience: Four (4) years relevant IT experience. Possess one or more security related certifications.
Minimum Education: Highschool/GED

Intrusion Analyst
Functional Responsibility: Work with a team to provide day-to-day support to manage and perform active defense and prevention network security monitoring functions. Perform advanced data mining, event and correlation for IDS/IPS detected incidents and work with the Security Engineers to improve the teams overall detection/prevention capabilities. Provide technical analysis of network activity; the analyst monitors and evaluates network event data, signature-based IDS events and full packet capture (PCAP) data. Triage IDS alerts; collect related data from various network analysis systems, review available open and closed source information on related threats & vulnerabilities, prepare initial summary reports. Monitor and analyze signature-based IDS alerts and associated packet (PCAP) data. Analyze network flow data for anomalies and to correlate reporting with enterprise-wide network activity. Document key event details and analytic findings in an incident management system. Perform incident correlation & escalation. Communicate and collaborate with analysts from other SOC organizations to investigate cyber events. Assess cyber indicators/observables and collaborate in the development of IDS signatures and detection mechanisms. Monitor and report on trends and activity on network sensor platforms. Provide technical assessments of cyber threats and vulnerabilities. Develop, maintain and update standard operating procedures. Provide routine status updates for ongoing projects, trouble tickets, incidents, and other related tasks. Maintain awareness of major events and trends in the cyber security landscape. Ensure that all alerts are monitored, interpreted, analyzed, and investigated. Utilize

external reporting tools for threat intelligence. Monitor all security-relevant logs and alerts for signs of compromise, attack, or system misuse and policy violations. Write detailed incident reports. Collect incident and investigation metrics and trending data, identify key trends, and provide situational awareness on these trends. Monitor all-source threat reporting.
Minimum/General Experience: Two (2) years Intrusion Detection/Intrusion Prevention (IDS/IPS) experience. Possess one or more security related certifications.
Minimum Education: Highschool/GED

Managing Security Consultant
Functional Responsibility: Directs the Cybersecurity and IA teams in the delivery of information security, information security systems, and/or computer security requirements. Architects, assesses, develops, engineers and implements Cybersecurity solutions. Retrieves, gathers and organizes technical information about an organization's risks, vulnerabilities, and exposures within the existing security products, networks, applications, and programs. Develops, analyzes, and implements Cybersecurity architecture(s) as appropriate. Performs risk analysis assessments, conducts Cybersecurity governance and compliance services, develops analytical and technical reports as required. May be required to perform in one or more of the following areas: risk and vulnerability assessments; cyber hunting activities; conducting penetration testing and scanning; assessment of system security for compliance; security of computer network hardware; operating system utility/support software; disaster recovery; incident response and digital forensics; application assessment; vulnerability threat management; cloud security; contingency planning; social engineering; and the development of security policies and procedures. May be responsible for leading a team in performing these services.
Minimum/General Experience: Ten (10) years of experience. Must possess one or more security related certifications.
Minimum Education: Bachelor's degree for equivalent.

Risk/Vulnerability Analyst
Functional Responsibility: Provide expertise in vulnerability management processes and network vulnerability scanning. Configure network scans, schedule network scans to run with bandwidth use in mind, and ensure accurate vulnerability assessment results are generated and made available to appropriate personnel. Configure vulnerability assessment tools to perform vulnerability scanning on enterprise network. Troubleshoot issues arising from vulnerability scanning and serve as technical expert for vulnerability assessment tools.
Minimum/General Experience: Three (3) years providing vulnerability assessment and troubleshooting. Windows, UNIX, and Linux operating systems support experience.
Minimum Education: Bachelor's degree for equivalent.

Security Analyst
Functional Responsibility: Assisting member of a team for delivering on a specific Cybersecurity task of a small/simple projects individually and large projects as a team member with oversight and continual skill development.
Minimum/General Experience: Two (2) years of relevant experience.
Minimum Education: Highschool/GED

Security Consultant
Functional Responsibility: Assists more experienced consultants in analyzing and defining security requirements. Assists in performing risk analysis and security audit services and in developing analytical reports. May assist in performing in one or more of the following areas: Risk and Vulnerability Assessments; Cyber Hunting activities; conducting Penetration Testing and scanning; assessment of system security for compliance of applications; security of computer network hardware; operating system utility/support software; disaster recovery; incident response and digital forensics; application assessment; vulnerability threat management; cloud security; contingency planning; social engineering; and the development of security policies and procedures.
Minimum/General Experience: Two (2) years of relevant experience.
Minimum Education: Bachelor's degree or equivalent.

Senior Security Consultant
Functional Responsibility: Analyzes and defines security requirements and designs, develops, engineers, and implements solutions. Performs risk analysis and security audit services, developing analytical reports as required. May be required to perform in one or more of the following areas: risk and vulnerability assessments; cyber hunting activities; conducting penetration testing and scanning; assessment of system security for compliance; security of computer network hardware; operating system utility/support software; disaster recovery; incident response and digital forensics; application assessment; vulnerability threat management; cloud security; contingency planning; social engineering; and the development of security policies and procedures.
Minimum/General Experience: Six (6) years of relevant experience.
Minimum Education: Bachelor's degree or equivalent.

Senior Subject Matter Expert (SME)
Functional Responsibility: Provides insight and guidance to the client regarding their strategic Information Assurance systems plans, information security technology business goals and the client's cybersecurity management strategy. Analyzes and assesses client cybersecurity systems and architecture requirements and recommends development or acquisition strategies for security solutions. Assists clients in developing strategic cybersecurity plans and concepts. Advises client on the impact of new cybersecurity legislation, mandates, regulations or new technologies and industry best-practices that are relevant to their agency. Demonstrates superior oral and written communication skills.
Minimum/General Experience: Ten (10) years of relevant experience. Possesses requisite knowledge and expertise so recognized in the professional cybersecurity community that the individual is considered "expert" in the Information Assurance area being addressed. Advanced IA or IT certifications.
Minimum Education: Bachelor's degree or equivalent.

Task Order Project Manager
Functional Responsibility: Serves as the project manager for a large, complex task order (or a group of task orders affecting the same system) and shall assist the Program Manager in working with the Government Contracting Officer (KO), the task order level Task Order Managers, Government management personnel and customer agency representatives. Under the guidance of the Program Manager, responsible for the overall management of the specific task order(s) and ensuring that the technical solutions and schedules in the task order are implemented in a timely manner.
Minimum/General Experience: Five (5) years relevant experience and 5 years of leadership experience with progressively higher responsibility in the public and/or private sector in the IT and/or consulting fields.
Minimum Education: Bachelor's degree or equivalent.

Vulnerability Analyst
Functional Responsibility: Conducts application, network, and system vulnerability assessments, documentation, and consultation of corrective, remediation actions. Responsible for assessing IT systems and supporting processes to ensure assessments and mitigating controls are consistent federal guidelines and organizational risk tolerances. Responsible for engaging with various enterprise and business process owners for the documentation, evaluation, and monitoring of current practices that are utilized in performing vulnerability assessment services. This includes
Minimum/General Experience: Two (2) years of related experience in the development of methods to ensure the accurate identification, prioritization, and remediation of vulnerabilities.
Minimum Education: Highschool/GED

Vulnerability Manager
Functional Responsibility: Responsible for the leadership and facilitation of security vulnerability remediation and ensuring transparency across the Enterprise. Develops the processes and tools to make vulnerability management more efficient and to work with teams to set priorities. Acts as a subject matter expert, liaise with key business and technology stakeholders to ensure compliance expectations are realized in a timely manner.
Minimum/General Experience: Five (5) years of experience with emphasis on IT Security and technical solutions. Possesses requisite knowledge and expertise so recognized in the professional cybersecurity community that the individual is considered "expert" in the Information Assurance area being addressed.
Minimum Education: Bachelor's degree or equivalent.

NOTE: Unless otherwise stated within the individual labor category Minimum Education description, one year of additional and directly applicable work experience may be substituted for one year of college education. For example, four years of additional and directly applicable work experience may be substituted for a Bachelor Degree requirement.

Company Overview

Horizon Industries employs the most current technology for business-based solutions in the areas of information technology, logistics and transportation, software development, systems integration and web development services. Our expertise includes systems design and development, database design and development, systems related financial and economic analysis, ERP Implementation, web development and project management.

Horizon Industries service offerings have been organized into six major categories and staffed with highly qualified, experienced professionals and leaders in our profession. These resources, combined with our targeted service model structure, allow us to deliver the support you need, where you need it and when you need it.

Service Offerings

- Financial Modeling
- Economic Analysis
- e-Business Consulting
- Systems Design and Development
- ERP Implementation
- Systems Related Change Management

SIN 132-45B Incident Response GSA Pricing

Labor Category	Hourly Rate
Cyber Security Analyst	$108.27
Cyber Security Operations Manager	$135.53
Cyber Security Program Manager	$133.77
Cyber Security System Engineer	$108.27
Cyber Threat Intelligence Analyst	$108.27
Forensics Analyst	$108.27
Incident Response Analyst	$108.17
Intrusion Analyst	$108.17
Managing Security Consultant	$133.77
Security Analyst	$117.39
Security Consultant	$108.17
Senior Security Consultant	$132.39
Senior Subject Matter Expert (SME)	$133.77
Subject Matter Expert (SME)	$132.39
TOPM	$132.99

SIN 132-45C Cyber Hunt GSA Pricing

Labor Category	Hourly Rate
Cyber Security Analyst	$108.27
Cyber Security Operations Manager	$135.53
Cyber Security Program Manager	$133.77
Cyber Security System Engineer	$108.27
Cyber Threat Intelligence Analyst	$108.27
Forensics Analyst	$108.27
Incident Handler	$108.17
Incident Responder	$108.17
Incident Response Analyst	$108.17
Incident Response Coordinator	$108.27
Intrusion Analyst	$108.17
Managing Security Consultant	$133.77
Security Analyst	$117.39
Security Consultant	$108.17
Senior Security Consultant	$132.39
Senior Subject Matter Expert (SME)	$133.77
Subject Matter Expert (SME)	$132.39
TOPM	$132.99

SIN 132-45D Risk and Vulnerability Assessments (RVA GSA Pricing

Labor Category	Hourly Rate
Computer Network Defense (CND) Auditor	$108.27
Computer Security Systems Specialist	$135.53
Cyber Compliance Manager	$133.77
Cyber Security Analyst	$108.27
Cyber Security Operations Manager	$108.27
Cyber Security Program Manager	$108.27
Cyber Security System Engineer	$108.17
Cyber Threat Intelligence Analyst	$108.17
Ethical Hacker	$108.17
Forensics Analyst	$108.27
Information Assurance Security Engineer	$108.17
Managing Security Consultant	$133.77
Risk/Vulnerability Analyst	$117.39
Security Analyst	$108.17
Security Consultant	$132.39
Senior Security Consultant	$133.77
Senior Subject Matter Expert (SME)	$132.39
Subject Matter Expert (SME)	$132.99
TOPM	$131.99
Vulnerability Analyst	$116.50
Vulnerability Manager	$115.82

SIN 132-51 GSA Pricing

Labor Category	Hourly Rate
Documentation Specialist	$73.70
Program Analyst	$108.82
Program Manager	$165.04
Program Specialist	$104.44
Project Manager	$149.62
Senior IT Analyst/Designer	$174.56
Software Developer Consultant	$141.31
Sr. Developer Consultant	$141.31
Sr. Program Specialist	$136.90
Sr. Trainer/Facilitator	$353.79
Subject Matter Expert	$141.31
Systems Analyst	$135.50
Systems Developer	$120.18
Technical Writer	$51.69
Trainer/Facilititator	$198.91