GSA IT70 Schedule with SINS 132 51, IT Professional Services, SIN 132 45B Incident Response and SIN 132 45C Cyber Hunt

APPROVED

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

47QTCA18D00L5

Pricelist current and dated 10/26/2018

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

General Description

CoAspire, LLC was founded in 2013 and is based Fairfax, Virginia. CoAspire has been providing a broad array of Information Technology (IT) and Cybersecurity products and services related to this schedule to both federal and commercial customers since its founding.

Contract Number: 47QTCA18D00L5

Period Covered by Contract: *September 25, 2018 through September 24, 2023*

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- 45B, 132-45C 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 – IT Professional Services
- 132 45B – Incident Response
- 132 45C – Cyber Hunt

3. **Minimum Order:**

The Minimum Order for the following SINs is $100.00.

- 132 51 – IT Professional Services
- 132 45B – Incident Response
- 132 45C – Cyber Hunt

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, 132-45B, 132-45C	TBD between CoAspire and the ordering activity

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

    c. OVERNIGHT and TWO-DAY DELIVERY: As negotiated between CoAspire 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:

CoAspire, LLC
4031 University Drive, Ste. 100
Fairfax, Virginia 22030

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:

CoAspire, LLC
4031 University Drive, Ste. 100
Fairfax, Virginia 22030

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

703.915.0582
info@coaspire.com

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; info@coaspire.com

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

26. **Data Universal Numbering System (DUNS) Number:** 078735548

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 132-45B)

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 SIN 132-45B, and 132-45C 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. Description of Labor Categories

Job Titles	Functional Responsibilities	Minimum Education and 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 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
Network Engineer 2	Minimum 5 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, 5 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 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
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 (cont.)	Bachelor's degree < 1 year's experience

Job Titles	Functional Responsibilities	Minimum Education and Experience
	• 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	
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: • 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	Bachelor's degree, <5 years' experience
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 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, Updating, repairing, modifying, and expanding existing computer programs	Associate's degree < 5 years' experience

Job Titles	Functional Responsibilities	Minimum Education and Experience
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, < 5 years' experience
Cyber Security Specialist 1	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.	Bachelor's degree, 4 years' experience
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 routine aspects of the position and is supervised by higher levels.	Bachelors' 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. Performs more varied and difficult tasks compared to Level 1, yet has less autonomy than Level 3.	Bachelor's degree, 3 years' experience

Job Titles	Functional Responsibilities	Minimum Education and 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) •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
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	Bachelors' 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 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	Bachelor's degree, 10 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 5	$178.72
Program Manager 3	$118.49
Network Engineer 2	$126.39
Systems Architect 2	$111.58
Systems Integrator 1	$77.02
Incident Response Analyst 1	$62.21
Incident Response Analyst 2	$120.46
Security Operations Center (SOC) Analyst 4	$140.00
Cyber Programmer 1	$84.92
Cyber Programmer 2	$132.30
Cyber Security Specialist 1	$107.63
Cyber Security Specialist 2	$139.22
Cyber Security Specialist 3	$185.23
Cyber Hunter 1	$104.74
Cyber Hunter 2	$157.10
Cyber Hunter 3	$211.41
Cyber Hunter 4	$305.48