

I-FSS-600 CONTRACT PRICE LISTS

(i) GENERAL SERVICES ADMINISTRATION

Federal Supply Service

Authorized Federal Supply Schedule Price List

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

Schedule Title: *General Purpose Commercial Information Technology Equipment, Software and Services*

FSC Group *GSA IT70*, Part (NA), and Section or Standard Industrial Group (NA)

FSC Class(es)/Product code(s) and/or Service Codes (as applicable)

Contract number: *47QTCA18D00L8*

For more information on ordering from Federal Supply Schedules click on the FSS

Schedules button at fss.gsa.gov.

Contract period: *09/26/2018 – 09/25/2023*

Contractor's name, address, and phone number

Electrosoft Services, Inc. // 1893 Metro Center Dr. Suite 228; Reston, VA 20190 // (703)437-9451

Contractor's internet address/web site:

<https://www.electrosoft-inc.com>

Contract administration source:

Jose Arias, (703)437-9451 ext. 1017, jarias@electrosoft-inc.com

Business size: *Small Business; Woman-Owned Small Business (WOSB); Economically Disadvantaged Woman-Owned Small Business(EDWOSB); SBA Certified Small Disadvantaged business (SDB); SBA Certified 8(a) Firm (8a)*

(ii) CUSTOMER INFORMATION: The following information should be placed under this heading in consecutively numbered paragraphs in the sequence set forth below. If this information is placed in another part of the Federal Supply Schedule Price List, a table of contents must be shown on the cover page that refers to the exact location of the information.

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

<i>132-51</i>	<i>Information Technology Professional Services</i>
<i>132-45A</i>	<i>Penetration Testing Services</i>
<i>132-45B</i>	<i>Incident Response</i>
<i>132-45C</i>	<i>Cyber Hunt</i>
<i>132-45D</i>	<i>Risk and Vulnerability Assessment (RVA) Services</i>

1b. Identification of the lowest priced model number and lowest unit price for that model.

<i>132-51</i>	<i>\$52.77</i>
<i>132-45A-D</i>	<i>\$52.77</i>

1c. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles, experience, functional responsibility and education for those types of employees or subcontractors who will perform services shall be provided. If hourly rates are not applicable, indicate "Not applicable" for this item.

-Table included below-

2. Maximum order:	<i>132-51</i>	<i>\$500,000</i>
	<i>132-45A-D</i>	<i>\$500,000</i>

3. Minimum: *The minimum dollar of orders to be issued is \$ 100.00*
4. Geographic coverage (delivery area). *The Geographic Scope of Contract will be domestic delivery only including DC, HI, AK, and Puerto Rico.*
5. Point(s) of production (city, county, and State or foreign country). *1893 Metro Center Dr., Suite 228, Reston, VA 20190*
6. Discount from list prices or statement of net price: *Already deducted from the price.*
7. Quantity discounts: *None*
8. Prompt payment terms. Note: *0% Net 30 days*
- 9a. Notification that Government purchase cards are accepted at or below the micro-purchase threshold.
YES, Government Purchase Cards are accepted below the micro-purchase threshold.
- 9b. Notification whether Government purchase cards are accepted or not accepted above the micro-purchase threshold.
YES, Government Purchase Cards are accepted above the micro-purchase threshold.
10. Foreign items (list items by country of origin): *NA*
11. Time of delivery: *132-51 As negotiated Days*
132-45A-D As negotiated Days
12. F.O.B. point(s): *NA*
- 13a. Ordering address: *1893 Metro Center Dr. Suite 228 Reston, VA 20190*
- 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: *1893 Metro Center Dr. Suite 228 Reston, VA 20190*
15. Warranty provision: *30 day warranty*
16. Export: *NA*
17. Terms and conditions of Government purchase card acceptance: *No additional T&C's*
18. Terms and conditions of rental, maintenance, and repair: *NA*
19. Terms and conditions of installation: *NA*
20. Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices: *NA*
- 20a. Terms and conditions for any other services: *NA*
21. List of service and distribution points: *NA*
22. List of participating dealers: *NA*

23. Preventive maintenance: *NA*

24a. Special attributes such as environmental attributes: *None*

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 (*NA, None*) The EIT standards can be found at: www.Section508.gov/.

25. Data Universal Number System (DUNS) number: 02-2665041

26. Notification regarding registration in System for Award Management (SAM) database: *Active in (SAM)*

SPECIAL ITEM NUMBER 132-51 - INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES

FPDS Code D302 IT Systems Development Services

FPDS Code D306 IT Systems Analysis Services

FPDS Code D307 Automated Information Systems Design and Integration Services

FPDS Code D308 Programming Services

FPDS Code D310 IT Backup and Security Services

FPDS Code D399 Other Information Technology Services, Not Elsewhere Classified

Note 1: All non-professional labor categories must be incidental to and used solely to support hardware, software and/or professional services, and cannot be purchased separately.

Note 2: Offerors and Agencies are advised that the Group 70 – Information Technology Schedule is not to be used as a means to procure services which properly fall under the Brooks Act. These services include, but are not limited to, architectural, engineering, mapping, cartographic production, remote sensing, geographic information systems, and related services. FAR 36.6 distinguishes between mapping services of an A/E nature and mapping services which are not connected nor incidental to the traditionally accepted A/E Services.

Note 3: This solicitation is not intended to solicit for the reselling of IT Professional Services, except for the provision of implementation, maintenance, integration, or training services in direct support of a product. Under such circumstances the services must be performance by the publisher or manufacturer or one of their authorized agents.

TERMS AND CONDITIONS APPLICABLE TO INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 132-51)

1. SCOPE

- a. The prices, terms and conditions stated under Special Item Number 132-51 Information Technology Professional Services apply exclusively to IT/IAM 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 shall 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/IAM 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/IAM Professional Services.

9. INDEPENDENT CONTRACTOR

All IT/IAM 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/IAM 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/IAM PROFESSIONAL SERVICES AND PRICING

Commercial Job Title	Minimum/General Experience	Minimum Education	GSA Price with IFF
Chief Scientist	The Chief Scientist must have twelve years of progressive experience in the field of information security, must be nationally recognized in some aspect of information security, and must have published at least two technical papers in the area of information security in refereed technical journals or magazines. The individual must have at least five years of experience in providing technical leadership to information security projects.	The individual must have at least a Master's Degree in Computer Science or a related field.	\$164.03
Senior Security Engineer	The senior security engineer must have eight years of progressive experience in the field of information security. The individual must have at least two years of experience in providing technical leadership to information security projects.	The individual must have a Bachelor's Degree in Computer Science or related field.	\$156.09
Intermediate Security Engineer	The intermediate security engineer must have five years of progressive experience in the field of information security. The individual must have at least one year of experience in providing technical leadership to information security projects.	The individual must have a Bachelor's Degree in Computer Science or related field.	\$102.48
Security Engineer	The security engineer must have two years of experience in the field of information security.	The individual must have a Bachelors' degree in Computer Science or related field. A Masters in Computer Science or related field could be substituted for one year of experience.	\$91.10

Senior Systems Engineer	The Senior Systems Engineer must have seven years of experience in information systems engineering, and five years of experience in engineering large, complex systems or networks. The individual must have demonstrated experience in analytical problem solving of work flows, organization and planning.	A Master's Degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline.	\$127.00
Subject Matter Expert	The Subject Matter Expert must have eight years of experience in research and development, information systems engineering or information operations, and have demonstrated ability to apply principles and methods of information technology in problems dealing with information security and information assurance.	A Ph.D. Degree in Computer Science, Information Systems, Engineering, Business, Mathematics or other related scientific or technical discipline is required.	\$209.95
Intermediate Administrative Assistant	The Intermediate Administrative Assistant must have two years of experience in using a PC, Windows operating systems, and must know how to use popular software packages for word processing, spreadsheet, database, electronic mail, and presentations.	An Associate's Degree in Business or Information Systems or a Business School graduation or business related courses in Word Processing, Computer Graphics, Graphics Illustration or Administration.	\$53.17
Analyst I	0 years	Bachelor's Degree.	\$83.81
Analyst II	2 years supporting IT programs or systems	Bachelor's Degree	\$98.59
Consultant I	4 years supporting IT programs or systems	Bachelor's Degree	\$114.86
Consultant II	6 years supporting IT programs or systems	Bachelor's Degree	\$137.70
Senior Consultant	10 years supporting IT programs or systems	Master's Degree	\$180.38
Project Manager I	6 years supporting IT programs or systems with 1 year as a Project Manager	Bachelor's Degree with PMP Certification preferred	\$123.23
Project Manager II	8 years supporting IT programs or systems with 2 years as a Project Manager	Bachelor's Degree with PMP Certification	\$138.79
Program Manager I	10 years supporting IT programs or systems with 4 years as a Project Manager	Master's Degree with PMP certification	\$161.17
Program Manager II	15 years supporting IT programs or systems with 8 years as a Project Manager	Master's Degree with PMP certification	\$196.10

Documentation Specialist	4 years of documentation experience	Bachelor's Degree	\$80.73
Software Architect	9 years of directly related experience and 2 years of supervisory experience	Bachelor's Degree	\$160.64
Software Developer I	2 years of development experience	Bachelor's Degree	\$82.98
Software Developer II	4 years of development experience	Bachelor's Degree	\$119.86
Software Developer III	6 years of development experience	Bachelor's Degree	\$147.52
Software Engineer II	5 years supporting IT programs or systems as a developer	Bachelor's Degree	\$123.94
System Administrator I	1 year experience	Associates Degree or Technical Certification	\$78.87
System Administrator II	3 years of experience with some experience supervising others	Associates Degree or Technical Certification with Bachelor's Degree preferred	\$118.71
System Engineer I	5 years supporting IT programs or systems	Bachelor's Degree	\$100.57
System Engineer II	8 years supporting IT programs or systems	Bachelor's Degree	\$123.22

***For all positions 2 years of additional experience can substitute for an Associate's Degree, 4 years of additional experience can substitute for a Bachelor's Degree, and 2 years of additional experience can substitute for a Master's Degree.**

SPECIAL ITEM NUMBER 132-45 Highly Adaptive Cybersecurity Services (HACS)

Subject to Cooperative Purchasing includes proactive and reactive cybersecurity services that improve the customer's enterprise-level security posture.

The scope of this category encompasses a wide range of fields that include, but are not limited to, Risk Management Framework (RMF) services, information assurance (IA), virus detection, network management, situational awareness and incident response, secure web hosting, and backup and security services.

The scope of this category also includes Security Operations Center (SOC) services. HACS vendors are able to identify and protect a customer's information resources, detect and respond to cybersecurity events or incidents, and recover capabilities or services impaired by any incidents that emerge.

Sub-Categories

- High Value Asset (HVA) Assessments
- Risk and Vulnerability Assessment (RVA)
- Cyber Hunt
- Incident Response
- Penetration Testing

**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
- 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.

The following is an example of the manner in which the description of a commercial job title should be

presented (see SCP FSS 004)

EXAMPLE

Commercial Job Title: Computer Network Defense Analysis

Description: Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

Professionals involved in this specialty perform the following tasks:

- Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities
- Provide daily summary reports of network events and activity relevant to Computer Network Defense practices
- Monitor external data sources (e.g., Computer Network Defense vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of Computer Network Defense threat condition and determine which security issues may have an impact on the enterprise.

Knowledge, Skills and Abilities: Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws, etc.), statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed

Minimum Experience: 5 Years

Minimum Education Requirements: a bachelor's of science degree with a concentration in computer science, cybersecurity services, management information systems (MIS), engineering or information science is essential.

Highly Desirable: Offensive Security Certified Professional (OSCP) or commercial Cybersecurity advanced certification(s).

Commercial Job Title	Minimum/General Experience	Minimum Education	GSA Price with IFF
Chief Scientist	The Chief Scientist must have twelve years of progressive experience in the field of information security, must be nationally recognized in some aspect of information security, and must have published at least two technical papers in the area of information security in refereed technical journals or magazines. The individual must have at least five years of experience in providing technical leadership to information security projects.	The individual must have at least a Master's Degree in Computer Science or a related field.	\$164.03

Senior Security Engineer	The senior security engineer must have eight years of progressive experience in the field of information security. The individual must have at least two years of experience in providing technical leadership to information security projects.	The individual must have a Bachelor's Degree in Computer Science or related field.	\$156.09
Intermediate Security Engineer	The intermediate security engineer must have five years of progressive experience in the field of information security. The individual must have at least one year of experience in providing technical leadership to information security projects.	The individual must have a Bachelor's Degree in Computer Science or related field.	\$102.48
Security Engineer	The security engineer must have two years of experience in the field of information security.	The individual must have a Bachelors' degree in Computer Science or related field. A Masters in Computer Science or related field could be substituted for one year of experience.	\$91.10
Senior Systems Engineer	The Senior Systems Engineer must have seven years of experience in information systems engineering, and five years of experience in engineering large, complex systems or networks. The individual must have demonstrated experience in analytical problem solving of work flows, organization and planning.	A Master's Degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline.	\$127.00
Subject Matter Expert	The Subject Matter Expert must have eight years of experience in research and development, information systems engineering or information operations, and have demonstrated ability to apply principles and methods of information technology in problems dealing with information security and information assurance.	A Ph.D. Degree in Computer Science, Information Systems, Engineering, Business, Mathematics or other related scientific or technical discipline is required.	\$209.95
Intermediate Administrative Assistant	The Intermediate Administrative Assistant must have two years of experience in using a PC, Windows operating systems, and must know how to use popular software packages for word processing, spreadsheet, database, electronic mail, and presentations.	An Associate's Degree in Business or Information Systems or a Business School graduation or business related courses in Word Processing, Computer Graphics, Graphics Illustration or Administration.	\$53.17
Analyst I	0 years	Bachelor's Degree.	\$83.81
Analyst II	2 years supporting IT programs or systems	Bachelor's Degree	\$98.59
Consultant I	4 years supporting IT programs or systems	Bachelor's Degree	\$114.86

Consultant II	6 years supporting IT programs or systems	Bachelor's Degree	\$137.70
Senior Consultant	10 years supporting IT programs or systems	Master's Degree	\$180.38
Project Manager I	6 years supporting IT programs or systems with 1 year as a Project Manager	Bachelor's Degree with PMP Certification preferred	\$123.23
Project Manager II	8 years supporting IT programs or systems with 2 years as a Project Manager	Bachelor's Degree with PMP Certification	\$138.79
Program Manager I	10 years supporting IT programs or systems with 4 years as a Project Manager	Master's Degree with PMP certification	\$161.17
Program Manager II	15 years supporting IT programs or systems with 8 years as a Project Manager	Master's Degree with PMP certification	\$196.10
Documentation Specialist	4 years of documentation experience	Bachelor's Degree	\$80.73