GENERAL SERVICES ADMINISTRATION
FEDERAL SUPPLY SERVICE
AUTHORIZED FEDERAL SUPPLY SCHEDULE CATALOG/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 is available through GSA Advantage!, a menu-driven database system. The INTERNET address for GSA Advantage! is http://www.gsaadvantage.gov

SCHEDULE TITLE: Multiple Award Schedule (MAS)
Federal Supply Group: Information Technology

CONTRACT NUMBER: 47QTCA21D00C4

CONTRACT PERIOD: July 12, 2021 through July 11, 2026
Pricelist current through Mod PS-A832

Contractor:
Zephon LLC
9112 Garden Grove Dr
McKinney, TX 75072
Phone: 469-343-4371
Website: www.zephon.tech

Contract Administrator: Vishal Masih
Email: vmasih@zephon.tech

DUNS: 100502794
NAICS Code(s): 541512, 541513, 541519, 541511


FSC Classes/Product Codes: DJ01 - IT and Telecom - Security and Compliance Support Services (Labor)

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

1.0 Information for Ordering Activities ............................................................................................................ 3
2.0 Terms and Conditions Applicable to Highly Adaptive Cybersecurity Services (HACS) (SIN 54151HACS) ........................................................................................................................................ 6
3.0 Labor Category Pricing .................................................................................................................................... 11
4.0 Labor Category Descriptions .......................................................................................................................... 12
5.0 OLM Information ........................................................................................................................................... 14
1.0 Information for Ordering Activities

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

<table>
<thead>
<tr>
<th>SINs</th>
<th>Recovery</th>
<th>SIN Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HACS</td>
<td>54151HACSRC</td>
<td>Highly Adaptive Cybersecurity Services (HACS)</td>
</tr>
<tr>
<td>OLM</td>
<td>OLMRC</td>
<td>ORDER-LEVEL MATERIALS (OLM)</td>
</tr>
</tbody>
</table>

1b. Identification of the lowest priced model number and lowest unit price for that model for each special item number awarded in the contract. This price is the Government price based on a unit of one, exclusive of any quantity/dollar volume, prompt payment, or any other concession affecting price. Those contracts that have unit prices based on the geographic location of the customer, should show the range of the lowest price, and cite the areas to which the prices apply. See Page 11.

1c. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles, experience, functional responsibility, and education for those types of employees or subcontractors who will perform services shall be provided. If hourly rates are not applicable, indicate “Not applicable” for this item. See Page 11.

2. Maximum order: $500,000

3. Minimum order: $100

4. Geographic coverage (delivery area). Domestic; 50 States, DC and Territories.

5. Point(s) of production (city, county, and State or foreign country). 9112 Garden Grove Drive, McKinney, TX 75072-4946


7. Quantity discounts. 1.5% equal to or greater than $150,000.

8. Prompt payment terms. Information for Ordering Offices: Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions. 1.0% if Payment is made within 7 Days.

10a. Time of delivery. Contact Contractor or To Be Determined at the Task Order level.

10b. Expedited Delivery. Items available for expedited delivery are noted in this price list. Contact Contractor or To Be Determined at the Task Order level.

10c. Overnight and 2-day delivery. Contact Contractor or To Be Determined at the Task Order level.

10d. Urgent Requirements. Contact Contractor or To Be Determined at the Task Order level.

11. F.O.B. point(s). Destination.

12a. Ordering address(es). 9112 Garden Grove Drive, McKinney, TX 75072-4946

12b. 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.

13. Payment address(es). 9112 Garden Grove Drive, McKinney, TX 75072-4946


15. Export packing charges, if applicable. Not Applicable.

16. Terms and conditions of rental, maintenance, and repair (if applicable). Not Applicable.

17. Terms and conditions of installation (if applicable). Not Applicable.

18a. Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices (if applicable). Not Applicable.

18b. Terms and conditions for any other services (if applicable). Not Applicable.

19. List of service and distribution points (if applicable). Not Applicable.

20. List of participating dealers (if applicable). Not Applicable.

22a. Special attributes such as environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants). Not Applicable.

22b. 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/. Not Applicable.

23. Data Universal Number System (DUNS) number. 100502794

24. Cage Code. 8BEH7

25. Notification regarding registration in System for Award Management (SAM) database. Contractor registered and active in SAM. SAM Unique Entity ID: QX54CCLJ6F55
2.0 Terms and Conditions Applicable to Highly Adaptive Cybersecurity Services (HACS) (SIN 54151HACS)

54151HACS includes a wide range of fields such as, the seven-step Risk Management Framework services, information assurance, virus detection, network management, situational awareness and incident response, secure web hosting, and backup, security services and, Security Operations Center (SOC) services. HACS vendors are cataloged under the 5 subcategories of High Value Asset Assessments; Risk and Vulnerability Assessments, Cyber Hunt, Incident Response, and Penetration Testing.

Vendor suitability for offering services through the Highly Adaptive Cybersecurity Services (HACS) SIN 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-17-12 - Preparing for and Responding to a Breach of Personally Identifiable Information (PII)
- OMB Memorandum M- 19-03 - Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program
- 2017 Report to the President on Federal IT Modernization
- 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 800-44 - 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 800-160 - Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
• NIST SP 800-171 - Protecting Controlled Unclassified Information in non-federal Information Systems and Organizations

2.1 SCOPE
a. The labor categories, prices, terms and conditions stated under Special Item Number 54151HACS Highly Adaptive Cybersecurity Services (HACS) apply exclusively to Highly Adaptive Cybersecurity Services within the scope of this Multiple Award Schedule (MAS).
b. Services under this SIN are limited to Highly Adaptive Cybersecurity Services only. Software and hardware products are under different Special Item Numbers on Multiple Award Schedule (MAS) (e.g. 511210, 33411), and may be quoted along with services to provide a total solution.
c. This SIN provides ordering activities with access to Highly Adaptive Cybersecurity services only.
d. Highly Adaptive Cybersecurity Services provided under this SIN shall comply with all Cybersecurity certifications and industry standards as applicable pertaining to the type of services as specified by ordering agency.
e. SCOPE:

54151HACS 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 includes proactive and reactive cybersecurity services that improve customer enterprise-level security posture. Services 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. It 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 seven-step RMF includes preparation, information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. RMF activities may also include Information Security Continuous Monitoring Assessment (ISCMA) which evaluate organization wide ISCM implementations, and also Federal Incident Response Evaluations (FIREs), which assess an organization’s incident management functions.

The scope of this category also includes Security Operations Center (SOC) services. The SOC scope includes services such as: 24x7x365 monitoring and analysis, traffic analysis, incident response and coordination, penetration testing, anti-virus management, intrusion detection and prevention, and information sharing.
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.

This contract consists of the following subcategories under SIN 54151HACS:

- **High Value Asset (HVA)** Assessments include Risk and Vulnerability Assessment (RVA) which assesses threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations. The services offered in the RVA sub-category include Network Mapping, Vulnerability Scanning, Phishing Assessment, Wireless Assessment, Web Application Assessment, Operating System Security Assessment (OSSA), Database Assessment, and Penetration Testing. Security Architecture Review (SAR) evaluates a subset of the agency’s HVA security posture to determine whether the agency has properly architected its cybersecurity solutions and ensures that agency leadership fully understands the risks inherent in the implemented cybersecurity solution. The SAR process utilizes in-person interviews, documentation reviews, and leading practice evaluations of the HVA environment and supporting systems. SAR provides a holistic analysis of how an HVA’s individual security components integrate and operate, including how data is protected during operations. Systems Security Engineering (SSE) identifies security vulnerabilities and minimizes or contains risks associated with these vulnerabilities spanning the Systems Development Life Cycle. SSE focuses on but is not limited to the following security areas: perimeter security, network security, endpoint security, application security, physical security, and data security.

- **Risk and Vulnerability Assessment (RVA)** assesses threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations. The services offered in the RVA sub-category include Network Mapping, Vulnerability Scanning, Phishing Assessment, Wireless Assessment, Web Application Assessment, Operating System Security Assessment (OSSA), Database Assessment, and Penetration Testing.

- **Penetration Testing** is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network.

- **Incident Response** services help organizations impacted by a cybersecurity compromise determine the extent of the incident, remove the adversary from their systems, and restore their networks to a more secure state.

- **Cyber Hunt** activities respond to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Cyber Hunts start with the premise that threat actors known to target some organizations in a specific industry or with specific systems are likely to also target other organizations in the same industry or with the same systems.

f. 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.
2.2 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.

2.3 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 the GSA City Pair Program for travel in support of any contracts. All travel will be agreed upon with the client prior to the Contractor’s travel.

2.4 Inspection of Services
Inspection of services is in accordance with 552.212-4 - CONTRACT TERMS AND CONDITIONS–COMMERCIAL ITEMS (Jan 2017) & (ALTERNATE I-Jan 2017) for Time-and-Materials and Labor-Hour orders placed under this contract.

2.5 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.

2.6 Responsibilities of the Ordering Activity
Subject to the ordering activity security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite Highly Adaptive Cybersecurity Services.
2.7 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.

2.8 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.

2.9 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.

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

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

2.12 Description of Highly Adaptive Cybersecurity Services and Pricing
Please refer to the labor category description and pricing incorporated into this price

GSA SCHEDULE # 47QSMD20R0001
Contract # 47QTCA21D00C4

Zephon LLC
3.0 Labor Category Pricing

Highly Adaptive Cybersecurity Services (SIN 54151HACS)  
(Pricing with IFF)

<table>
<thead>
<tr>
<th>LABOR CATEGORY</th>
<th>Base - Year 1 (07/12/2021 - 07/11/2022)</th>
<th>Year 2 (07/12/2022 - 07/11/2023)</th>
<th>Year 3 (07/12/2023 - 07/11/2024)</th>
<th>Year 4 (07/12/2024 - 07/11/2025)</th>
<th>Year 5 (07/12/2025 - 07/11/2026)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Engineer</td>
<td>$117.88</td>
<td>$120.83</td>
<td>$123.85</td>
<td>$126.95</td>
<td>$130.12</td>
</tr>
<tr>
<td>Software Developer</td>
<td>$117.88</td>
<td>$120.83</td>
<td>$123.85</td>
<td>$126.95</td>
<td>$130.12</td>
</tr>
<tr>
<td>Sr. Software Developer</td>
<td>$147.36</td>
<td>$151.04</td>
<td>$154.82</td>
<td>$158.69</td>
<td>$162.65</td>
</tr>
<tr>
<td>Security Consultant</td>
<td>$113.95</td>
<td>$116.80</td>
<td>$119.72</td>
<td>$122.72</td>
<td>$125.78</td>
</tr>
</tbody>
</table>

*Annual fixed escalation rate of 2.5%*

**Service Contract Labor Standards:** Not applicable.
## 4.0 Labor Category Descriptions

### Security Engineer

<table>
<thead>
<tr>
<th>Minimum Education:</th>
<th>Bachelor’s Degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Years’ Experience:</td>
<td>Two (2) years</td>
</tr>
</tbody>
</table>

**Responsibilities:**
- Implement security controls and vulnerability remediations
- Perform security testing and hardening
- Identify security issues
- Develop tools and utilities as needed
- Security systems integrations and implementations

### Software Developer

<table>
<thead>
<tr>
<th>Minimum Education:</th>
<th>Bachelor’s Degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Years’ Experience:</td>
<td>Two (2) years</td>
</tr>
</tbody>
</table>

**Responsibilities:**
- Develop software applications (web/mobile/systems)
- Individual or team contributor to application development and systems design and integration

### Sr. Software Developer

<table>
<thead>
<tr>
<th>Minimum Education:</th>
<th>Bachelor’s Degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Years’ Experience:</td>
<td>Five (5) years</td>
</tr>
</tbody>
</table>

**Responsibilities:**
- Lead software development teams for entire projects or individual modules
- Review teams’ contribution for quality, security, and best practices
- Ensure timely delivery of assigned deliverables and sync with project management teams and lead architects
- Proactively identify issues and roadblocks in project execution
- Take ownership of assigned tasks and deliverables

### Security Consultant

<table>
<thead>
<tr>
<th>Minimum Education:</th>
<th>Bachelor’s Degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Years’ Experience:</td>
<td>One (1) year</td>
</tr>
</tbody>
</table>
Responsibilities:
- Document, track and present governance, risk and compliance policies and violations
- Work with security engineering team to ensure violations and vulnerabilities are rectified and remediated
- Develop tools and utilities as needed
- Security systems integrations and implementations

Experience Substitutions:

<table>
<thead>
<tr>
<th>High School Diploma + 2 years additional experience</th>
<th>Equals</th>
<th>Associate Degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associate Degree + 2 years additional experience</td>
<td>Equals</td>
<td>Bachelor's Degree</td>
</tr>
<tr>
<td>Bachelor's Degree + 2 years additional experience</td>
<td>Equals</td>
<td>Master's Degree</td>
</tr>
<tr>
<td>Master's Degree + 3 years additional experience</td>
<td>Equals</td>
<td>PhD</td>
</tr>
</tbody>
</table>

Education Substitutions:

<table>
<thead>
<tr>
<th>Minimum Education Requirement</th>
<th>Years of Experience Substitution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associate Degree</td>
<td>2 years</td>
</tr>
<tr>
<td>Bachelor's Degree</td>
<td>4 years</td>
</tr>
<tr>
<td>Master's Degree</td>
<td>6 years</td>
</tr>
</tbody>
</table>
5.0 OLM - SPECIAL ORDERING PROCEDURES FOR THE ACQUISITION OF ORDER-LEVEL MATERIALS (MAY 2019)

(a) Definition. "Order-level materials" means supplies and/or services acquired in direct support of an individual task or delivery order placed against a Federal Supply Schedule (FSS) contract or FSS blanket purchase agreement (BPA), when the supplies and/or services are not known at the time of Schedule contract or FSS BPA award. The prices of order-level materials are not established in the FSS contract or FSS BPA. Order-level materials acquired following the procedures in paragraph (d) of this section are done so under the authority of the FSS program, pursuant to 41 U.S.C. 152(3), and are not open market items, which are discussed in FAR 8.402(f).

(b) FAR 8.403(b) provides that GSA may establish special ordering procedures for a particular FSS.

(c) The procedures in FAR subpart 8.4 apply to this contract, with the exceptions listed in this clause. If a requirement in this clause is inconsistent with FAR subpart 8.4, this clause takes precedence pursuant to FAR 8.403(b).

(d) Procedures for including order-level materials when placing an individual task or delivery order against an FSS contract or FSS BPA.

1. The procedures discussed in FAR 8.402(f) do not apply when placing task and delivery orders that include order-level materials.

2. Order-level materials are included in the definition of the term "material" in FAR clause 52.212-4 Alternate I, and therefore all provisions of FAR clause 52.212-4 Alternate I that apply to "materials" also apply to order-level materials. The ordering activity shall follow procedures under the Federal Travel Regulation and FAR Part 31 when order-level materials include travel.

3. Order-level materials shall only be acquired in direct support of an individual task or delivery order and not as the primary basis or purpose of the order.

4. The value of order-level materials in a task or delivery order, or the cumulative value of order-level materials in orders against an FSS BPA awarded under a FSS contract shall not exceed 33.33%.

5. All order-level materials shall be placed under the Order-Level Materials SIN.
(6) Prior to the placement of an order that includes order-level materials, the Ordering Activity shall follow procedures in FAR 8.404(h).

(7) To support the price reasonableness of order-level materials—
   (i) The contractor proposing order-level materials as part of a solution shall obtain a minimum of three quotes for each order-level material above the simplified acquisition threshold.
      (A) One of these three quotes may include materials furnished by the contractor under FAR 52.212-4 Alt I (i)(1)(ii)(A).
      (B) If the contractor cannot obtain three quotes, the contractor shall maintain its documentation of why three quotes could not be obtained to support their determination.
      (C) A contractor with an approved purchasing system per FAR 44.3 shall instead follow its purchasing system requirement and is exempt from the requirements in paragraphs (d)(7)(i)(A)-(B) of this clause.
   (ii) The Ordering Activity Contracting Officer must make a determination that prices for all order-level materials are fair and reasonable. The Ordering Activity Contracting Officer may base this determination on a comparison of the quotes received in response to the task or delivery order solicitation or other relevant pricing information available.
   (iii) If indirect costs are approved per FAR 52.212-4(i)(1)(ii)(D)(2) Alternate I), the Ordering Activity Contracting Officer must make a determination that all indirect costs approved for payment are fair and reasonable. Supporting data shall be submitted in a form acceptable to the Ordering Activity Contracting Officer.

(8) Prior to an increase in the ceiling price of order-level materials, the Ordering Activity Contracting Officer shall follow the procedures at FAR 8.404(h)(3)(iv).

(9) In accordance with GSAR clause 552.238-83, Examination of Records by GSA, GSA has the authority to examine the Contractor’s records for compliance with the pricing provisions in FAR clause 52.212-4 Alternate I, to include examination of any books, documents, papers, and records involving transactions related to the contract for overbillings, billing errors, and compliance with the IFF and the Sales Reporting clauses of the contract.

(10) OLMs are exempt from the following clauses:
   (i) 552.216-70 Economic Price Adjustment - FSS Multiple Award Schedule Contracts.
   (ii) 552.238-77 Submission and Distribution of Authorized FSS Schedule Pricelists.
   (iii) 552.238-81 Price Reductions.
(11) Exceptions for travel.
   (i) Travel costs are governed by FAR 31.205-46 and therefore, the requirements in paragraph (d)(7) do not apply to travel costs.
   (ii) Travel costs do not count towards the 33.33% limitation described in paragraph (d)(4) of this section.
   (iii) Travel costs are exempt from clause 552.238-80 Industrial Funding Fee and Sales Reporting.