



GENERAL SERVICES ADMINISTRATION
Federal Supply Service
Authorized Federal Supply Schedule Price List
47QSMD20R0001

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 for GSA Advantage! is: GSAAdvantage.gov.

Schedule 70
General Purpose Commercial
Information Technology Equipment,
Software and Services

Special Item No. 54151S Information Technology Professional Services
Special Item No. 54151HACS Highly Adaptive Cybersecurity Services (HACS)

Contract Number: GS-35F-424DA

Period Covered by Contract: July 22, 2016 through July 21, 2021

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

Contractor:

Zen Strategics, LLC
10693 Water Falls Lane
Vienna, Virginia 22182
Phone (703) 587-8368
Fax (703) 713-0595
www.zenstrategics.com

Business Size: Small

Customer Information:

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

SIN: 54151S Information Technology (IT) Professional Services

SIN: 54151HACS Highly Adaptive Cybersecurity Services (HACS)

SIN: 518210ERM Electronic Records Management

1b. Identification of the lowest priced model number and lowest unit price for that model for each special item number awarded in the contract. N/A



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.

See Attachment A for Labor Category Descriptions.

LABOR CATEGORY	RATE W/IFF 2016- 2017 (\$)	RATE W/IFF 2017- 2018 (\$)	RATE W/IFF 2018- 2019 (\$)	RATE W/IFF 2019- 2020 (\$)	RATE W/IFF 2020- 2021 (\$)
<i>Program Manager</i>	134.89	137.58	140.34	143.14	146.01
<i>Security Analyst</i>	78.08	79.64	81.23	82.85	84.51
<i>Enterprise Architect</i>	119.90	122.29	124.74	127.23	129.78
<i>Network Engineer</i>	112.41	114.65	116.95	119.29	121.67
<i>IT Consultant Senior</i>	112.41	114.65	116.95	119.29	121.67
<i>IT Security Assessment Specialist</i>	112.41	114.65	116.95	119.29	121.67
<i>Documentation Specialist</i>	116.90	119.24	121.62	124.06	126.54
<i>IT Senior INFOSEC Engineer</i>	130.39	133.00	135.66	138.37	141.14
<i>Cloud SME/Program Manager</i>					216.53
<i>IT Senior Subject Matter Expert</i>					203.95
<i>Senior Penetration Tester</i>		161.21	164.43	167.72	171.08
<i>Mid-Level Penetration Tester</i>		130.98	133.60	136.27	139.00
<i>Senior Incident Response Analyst</i>		161.21	164.43	167.72	171.08
<i>Mid-Level Incident Response Analyst</i>		130.98	133.60	136.27	139.00
<i>Senior Risk & Vulnerability Analyst</i>		161.21	164.43	167.72	171.08
<i>Mid-Level Risk & Vulnerability Analyst</i>		130.98	133.60	136.27	139.00
<i>Cyber Subject Matter Authority</i>					247.03
<i>Senior Cyber Security Engineer</i>					218.31
<i>Senior Cyber Hunt Analyst</i>				161.21	164.43
<i>Mid-Level Cyber Hunt Analyst</i>				130.98	133.60
<i>Data Entry Supervisor</i>					94.71
<i>Quality Assurance Specialist</i>					98.97
<i>Records Manager I</i>					80.60
<i>Records Management Consultant</i>					113.65
<i>Subject Matter Expert II</i>					103.70
<i>Subject Matter Expert I</i>					135.13
<i>Records Manager III</i>					94.61
<i>Records Manager II</i>					84.99
<i>Records Management Associate</i>					73.48
<i>Records Clerk</i>					43.49

2. Maximum order. \$500,000.00

3. Minimum order. \$100.00

4. Geographic coverage (delivery area). Domestic, 50 states, Washington, DC, Puerto Rico, US Territories and to a CONUS port or consolidation point for orders received from overseas activities or give details as negotiated.

5. Point(s) of production (city, county, and State or foreign country). N/A



6. Discount from list, prices or statement of net price. Basic discount of 10%-15% from the awarded commercial price list.
7. Quantity discounts. 1% for \$100K, 2% for \$300K, 5% for \$500K
8. Prompt payment terms. 1%/20 Days; Net 30
- 9a. Notification that Government purchase cards are accepted at or below the micro-purchase threshold. Government Purchase Cards must be accepted at or below the micro-purchase threshold.
- 9b. Notification whether Government purchase cards are accepted or not accepted above the micro-purchase threshold. Contact contractor for limit.
10. Foreign items (list items by country of origin) N/A 11a.
Time of delivery. As negotiated per task order.
- 11b. Expedited Delivery. Items available for expedited delivery are noted in this price list.
- 11c. Overnight and 2-day delivery. Overnight and 2-day delivery are available. Contact the Contractor for rates.
- 11d. Urgent Requirements. Agencies can contact the Contractor's representative to affect a faster delivery. Customers are encouraged to contact the contractor for the purpose of requesting accelerated delivery.
12. F.O.B. point(s). Destination.
- 13a. Ordering address(es). Same as contractor address.
- 13b. Ordering procedures: For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPAs), and a sample EPA can be found at the GSA/FSS Schedule homepage (fss.gsa.gov/schedules).
14. Payment address(es): Same as contractor address.
15. Warranty provision. N/A
16. Export packing charges, if applicable. N/A
17. Terms and conditions of Government purchase card acceptance (any thresholds above the micro-purchase level) N/A
18. Terms and conditions of rental, maintenance, and repair (if applicable) N/A
19. Terms and conditions of installation (if applicable). N/A
20. Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices (if applicable). N/A
- 20a. Terms and conditions for any other services (if applicable) N/A
21. List of service and distribution points (if applicable). N/A
22. List of participating dealers (if applicable). N/A
23. Preventive maintenance (if applicable). N/A
- 24a. Special attributes such as environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants) N/A
- 24b. If applicable, indicate that Section 508 compliance information is available on Electronic and Information Technology (EIT) supplies and services and show where full details can be found (e.g. contractor's website or other location.) The EIT standards can be found at



www.Section508.gov/. N/A

25. Data Universal Number System (DUNS) number. 060621548

26. Notification regarding registration in System for Award Management database. Contractor has an Active Registration in the SAM database.

**TERMS AND CONDITIONS APPLICABLE TO INFORMATION TECHNOLOGY (IT)
PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 54151S)**

1. SCOPE

- a. The prices, terms and conditions stated under Special Item Number 54151S Information Technology Professional Services apply exclusively to IT Professional Services within the scope of this Information Technology Schedule.
- b. The Contractor shall provide services at the Contractor's facility and/or at the ordering activity location, as agreed to by the Contractor and the ordering activity.

2. PERFORMANCE INCENTIVES I-FSS-60 Performance Incentives (April 2000)

- a. Performance incentives may be agreed upon between the Contractor and the ordering activity on individual fixed price orders or Blanket Purchase Agreements under this contract.
- b. The ordering activity must establish a maximum performance incentive price for these services and/or total solutions on individual orders or Blanket Purchase Agreements.
- c. Incentives should be designed to relate results achieved by the contractor to specified targets. To the maximum extent practicable, ordering activities shall consider establishing incentives where performance is critical to the ordering activity's mission and incentives are likely to motivate the contractor. Incentives shall be based on objectively measurable tasks.

3. ORDER

- a. Agencies may use written orders, EDI orders, blanket purchase agreements, individual purchase orders, or task orders for ordering services under this contract. Blanket Purchase Agreements shall not extend beyond the end of the contract period; all services and delivery shall be made and the contract terms and conditions shall continue in effect until the completion of the order. Orders for tasks which extend beyond the fiscal year for which funds are available shall include FAR 52.232-19 (Deviation – May 2003) Availability of Funds for the Next Fiscal Year. The purchase order shall specify the availability of funds and the period for which funds are available.
- b. All task orders are subject to the terms and conditions of the contract. In the event of conflict between a task order and the contract, the contract will take precedence.

4. PERFORMANCE OF SERVICES

- a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity.
- b. The Contractor agrees to render services only during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.
- c. The ordering activity should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and



workmanlike manner.

d. Any Contractor travel required in the performance of IT Services must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel. Contractors cannot use GSA city pair contracts.

5. STOP-WORK ORDER (FAR 52.242-15) (AUG 1989)

(a) The Contracting Officer may, at any time, by written order to the Contractor, require the Contractor to stop all, or any part, of the work called for by this contract for a period of 90 days after the order is delivered to the Contractor, and for any further period to which the parties may agree. The order shall be specifically identified as a stop-work order issued under this clause. Upon receipt of the order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the order during the period of work stoppage. Within a period of 90 days after a stop-work is delivered to the Contractor, or within any extension of that period to which the parties shall have agreed, the Contracting Officer shall either-

(1) Cancel the stop-work order; or

(2) Terminate the work covered by the order as provided in the Default, or the Termination for Convenience of the Government, clause of this contract.

(b) If a stop-work order issued under this clause is canceled or the period of the order or any extension thereof expires, the Contractor shall resume work. The Contracting Officer shall make an equitable adjustment in the delivery schedule or contract price, or both, and the contract shall be modified, in writing, accordingly, if-

(1) The stop-work order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this contract; and

(2) The Contractor asserts its right to the adjustment within 30 days after the end of the period of work stoppage; provided, that, if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon the claim submitted at any time before final payment under this contract.

(c) If a stop-work order is not canceled and the work covered by the order is terminated for the convenience of the Government, the Contracting Officer shall allow reasonable costs resulting from the stop-work order in arriving at the termination settlement.

(d) If a stop-work order is not canceled and the work covered by the order is terminated for default, the Contracting Officer shall allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop-work order.

6. INSPECTION OF SERVICES

In accordance with FAR 52.212-4 CONTRACT TERMS AND CONDITIONS-- COMMERCIAL ITEMS (MAR 2009) (DEVIATION I - FEB 2007) for Firm-Fixed Price orders and FAR 52.212-4 CONTRACT TERMS AND CONDITIONS □ COMMERCIAL ITEMS (MAR 2009) (ALTERNATE I □ □ OCT 2008) (DEVIATION I – FEB 2007) applies to Time-and-Materials and Labor-Hour Contracts orders placed under this contract.

7. RESPONSIBILITIES OF THE CONTRACTOR



The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character. If the end product of a task order is software, then FAR 52.227-14 (Dec 2007) Rights in Data – General, may apply.

8. RESPONSIBILITIES OF THE ORDERING ACTIVITY

Subject to security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite IT Professional Services.

9. INDEPENDENT CONTRACTOR

All IT Professional Services performed by the Contractor under the terms of this contract shall be as an independent Contractor, and not as an agent or employee of the ordering activity.

10. ORGANIZATIONAL CONFLICTS OF INTEREST

a. Definitions.

“Contractor” means the person, firm, unincorporated association, joint venture, partnership, or corporation that is a party to this contract.

“Contractor and its affiliates” and “Contractor or its affiliates” refers to the Contractor, its chief executives, directors, officers, subsidiaries, affiliates, subcontractors at any tier, and consultants and any joint venture involving

the Contractor, any entity into or with which the Contractor subsequently merges or affiliates, or any other successor or assignee of the Contractor.

An “Organizational conflict of interest” exists when the nature of the work to be performed under a proposed ordering activity contract, without some restriction on ordering activities by the Contractor and its affiliates, may either (i) result in an unfair competitive advantage to the Contractor or its affiliates or (ii) impair the Contractor’s or its affiliates’ objectivity in performing contract work.

b. To avoid an organizational or financial conflict of interest and to avoid prejudicing the best interests of the ordering activity, ordering activities may place restrictions on the Contractors, its affiliates, chief executives, directors, subsidiaries and subcontractors at any tier when placing orders against schedule contracts. Such restrictions shall be consistent with FAR 9.505 and shall be designed to avoid, neutralize, or mitigate organizational conflicts of interest that might otherwise exist in situations related to individual orders placed against the schedule contract. Examples of situations, which may require restrictions, are provided at FAR 9.508.

11. INVOICES

The Contractor, upon completion of the work ordered, shall submit invoices for IT Professional services. Progress payments may be authorized by the ordering activity on individual orders if appropriate. Progress payments shall be based upon completion of defined milestones or interim products. Invoices shall be submitted monthly for recurring services performed during the preceding month.

12. PAYMENTS

For firm-fixed price orders the ordering activity shall pay the Contractor, upon submission of proper invoices or vouchers, the prices stipulated in this contract for service rendered and accepted. Progress payments shall be made only when authorized by the order. For time-and-materials orders, the Payments under Time-and-Materials and Labor-Hour Contracts at FAR 52.212-4 (MAR



2009) (ALTERNATE I – OCT 2008) (DEVIATION I – FEB 2007)

applies to time-and-materials orders placed under this contract. For labor-hour orders, the Payment under Time-and-Materials and Labor-Hour Contracts at FAR 52.212-4 (MAR 2009)

(ALTERNATE I – OCT 2008)

(DEVIATION I – FEB 2007) applies to labor-hour orders placed under this contract. 52.216-31(Feb 2007) Time- and-Materials/Labor-Hour Proposal Requirements—Commercial Item Acquisition As prescribed in 16.601(e)(3), insert the following provision:

- (a) The Government contemplates award of a Time-and-Materials or Labor-Hour type of contract resulting from this solicitation.
- (b) The offeror must specify fixed hourly rates in its offer that include wages, overhead, general and administrative expenses, and profit. The offeror must specify whether the fixed hourly rate for each labor category applies to labor performed by—
 - (1) The offeror;
 - (2) Subcontractors; and/or
 - (3) Divisions, subsidiaries, or affiliates of the offeror under a common control.

13. RESUMES

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

14. INCIDENTAL SUPPORT COSTS

Incidental support costs are available outside the scope of this contract. The costs will be negotiated separately with the ordering activity in accordance with the guidelines set forth in the FAR.

15. APPROVAL OF SUBCONTRACTS

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

16. DESCRIPTION OF IT PROFESSIONAL SERVICES AND PRICING

- a. The Contractor shall provide a description of each type of IT Service offered under Special Item Numbers 54151S IT Professional Services should be presented in the same manner as the Contractor sells to its commercial and other ordering activity customers. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles (labor categories) for those individuals who will perform the service should be provided.
- b. Pricing for all IT Professional Services shall be in accordance with the Contractor's customary commercial practices; e.g., hourly rates, monthly rates, term rates, and/or fixed prices, minimum general experience and minimum education.

TERMS AND CONDITIONS APPLICABLE TO HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS)

(SPECIAL ITEM NUMBER 54151HACS)

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

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

******NOTE: All labor categories under the Special Item Number 54151S Information Technology Professional Services may remain under SIN 54151S unless the labor categories are specific to the Highly Adaptive Cybersecurity Services SINS.**

1. SCOPE

The labor categories, prices, terms and conditions stated under Special Item Number 54151HACS High Adaptive Cybersecurity Services apply exclusively to High Adaptive Cybersecurity Services within the scope of this Information Technology Schedule.

- a. 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 and may be quoted along with services to provide a total solution.
- b. These SINS provide ordering activities with access to Highly Adaptive Cybersecurity services only.
- c. Highly Adaptive Cybersecurity Services provided under these SINS shall comply with all Cybersecurity certifications and industry standards as applicable pertaining to the type of services as specified by ordering agency.
- d. 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



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.

- a. The Contractor agrees to render services during normal working hours, unless

otherwise agreed to by the Contractor and the ordering activity.

- b.** 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.
- c.** 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.

- 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 following labor categories are offered under Special Item Number 54151HACS for Highly Adaptive Cybersecurity.

See Attachment A for Labor Category Descriptions.



TERMS AND CONDITIONS APPLICABLE TO ELECTRONIC RECORDS
MANAGEMENT

(SPECIAL ITEM NUMBER 518210ERM)

Vendor Certification for Electronic Records Management Solutions

For the purposes of the MAS Solicitation, eleven (11) specific elements of Electronic Records Management (ERM) Services have been identified. These 11 elements are fully defined and the corresponding requirements are identified in the Universal Electronic Records Management Requirements attachment to the Solicitation. These requirements have been established and are administered by the National Archives & Records Administration (NARA).

*Vendors may provide any combination of the 11 elements of ERM Services; however, vendors must certify that they are capable of meeting all standards associated with the elements they propose by completing this certification. **Vendors must include a completed copy of this certification in their published GSA catalog to illustrate their ERM capabilities.***

[Offeror Name] ZEN STRATEGICS

[Address] 10693 WATER FALLS LN, VIENNA, VA 22182

Proposed Elements of Electronic Records Management Services:

[Select all that apply]

- Element 1 - Office Management Applications (formerly "Desktop Applications")
- Element 2 - Electronic Messages
- Element 3 - Social Media
- Element 4 - Cloud Services
- Element 5 - Websites
- Element 6 - Digital Media (Photo)
- Element 7 - Digital Media (Audio)
- Element 8 - Digital Media (Video)
- Element 9 - Structured Data (formerly "Databases")
- Element 10 - Shared Drives
- Element 11 - Engineering Drawings



Zen Strategics hereby certifies that we are capable of meeting all standards described in the solicitation and the Universal Electronic Records Management Requirements attachment for each of the sections of ERM Services we have proposed, as indicated above.

Venu Ayala

Digitally signed by Venu Ayala
Date: 2020.11.09 13:29:37 -05'00'

Offeror (To be signed only by **authorized principal**, with authority to bind the undersigned contractor)

Venu Ayala

President

11/9/2020

Name (Printed)

Title

Date

Attachment A – Labor Category Descriptions

SIN 54151S

Program Manager
Education: B.A. or B.S. degree
Minimum Experience: Must have 12 years of IT experience, including at least 8 years of IT and/or telecommunications system management experience
Specialized Experience: At least 8 years of direct supervision of IT software development, integration, maintenance projects, and/or telecommunications systems. Must be capable of leading projects that involve the successful management of teams composed of data processing and other information management professionals who have been involved in analysis, design, integration, testing, documenting, converting, extending, and implementing automated information and/or telecommunications systems.
Duties: Performs day-to-day management of overall contract support operations, possibly involving multiple projects and groups of personnel at multiple locations. Organizes, directs, and coordinates the planning and production of all contract support activities. Demonstrates written and oral communication skills. Establishes and alters (as necessary) corporate management structure to direct effective contract support activities.
Security Analyst
Education: B.A. or B.S. or M.S. degree
Minimum Experience: Associates Degree with 2 years of related experience. Equivalents: High School diploma with four years of specialized experience in related field, or Bachelors or Master's Degree with no experience.
Specialized Experience: Serves as a senior member of consulting teams as a task manager or as a project leader on projects of limited scope and complexity. As a consulting team member, collects, analyzes, and interprets data in one or more information technology specialties. Develops, or participates in the development of, assignment methodology and coordinates with senior representatives within the customer organizations to address program goals, milestones, resources, and risks. Supports common user information systems, as well as dedicated special purpose systems requiring specialized security features and procedures.
Enterprise Architect
Education: MBA, M.S. or B.S. degree
Minimum Experience: Master's Degree or higher with 6 years of related experience. Equivalents: Bachelor's Degree from an accredited college or university with eight years' experience, or Doctorate Degree with four years' experience.
Specialized Experience: Establishes system information requirements using analysis from the information engineer(s) in the development of enterprise-wide or large-scale information systems. Designs architecture to include the software, hardware, and communications to support the total requirements, as well as provide for present and future cross-functional requirements and interfaces. As appropriate, ensures these systems are compatible and in compliance with the standards for open systems architectures; the Open Systems Interconnection (OSI) and International Standards Organization (ISO) reference models; and profiles of standards — such as Institute of Electrical and Electronic Engineers, Open Systems Environment, reference model — as they apply to the implementation and specification of Information Management solution of the application platform across the application program interface and external environment/software.

Network Engineer
Education: M.S. or B.S. degree
Minimum Experience: Bachelor's Degree from an accredited college or university with 5 years of related experience. Equivalents: High School diploma with nine years of specialized experience in related field, or Associates Degree with seven years of experience, or Master's Degree with three years' experience.
Specialized Experience: Provides support for technical direction and engineering expertise for communications (LAN/MAN/WAN) systems infrastructure activities, including network planning, designing, and implementing communications infrastructure requirements for buildings and systems. Ensures that adequate and appropriate planning is provided to direct building architects and planners in building communications spaces, networks, and media pathways to meet industry standards. Interfaces with internal and external customers and vendors to determine communications infrastructure needs.
IT Consultant Senior
Education: M.S. or B.S. degree
Basic Experience: Must have at least 8 years of experience, of which at least five must be specialized.
Specialized Experience: Manages the project work as defined by the client contract. Leads medium to large complex IT projects and major phases of very large projects. Manages the fact finding, analysis, and development of hypothesis/ conclusions, production of final reports and delivery of presentations. Responsible for ensuring that the project delivers to client expectations on time and to budget. Has expert knowledge of practice, consulting group, and matrixes organization operations and business objectives. Has in-depth knowledge of market/industry and service line.
IT Security Assessment Specialist
Education: M.S. or B.S. degree
Minimum Experience: Associates Degree with 2 years of related experience. Equivalents: High School diploma with four years of specialized experience in related field, or Bachelors or Master's Degree with no experience.
Specialized Experience: Establishes and satisfies system-wide information security requirements based upon the analysis of user, policy, regulatory, and resource demands. Provides leadership and guidance in the development, design, and application of solutions implemented by more junior staff members. Coordinates with senior representatives within the customer organizations to address program goals, milestones, resources, and risks. Supports common user information systems, as well as dedicated special purpose systems requiring specialized security features and procedures.
Documentation Specialist
Education: B.A. or B.S. degree
Minimum Experience: Experience: Requires an associate's degree in a related area and 2 years of experience in the field or in a related area.
Specialized Experience: Prepares and/or maintains documentation pertaining to programming, systems operation and user documentation. Translates business specifications into user documentation. Plans, writes, and maintains systems and user support documentation efforts, including online help screen. Has knowledge of commonly-used concepts, practices, and procedures within a particular field. Relies on instructions and pre-established guidelines to perform the functions of the job. Works under immediate supervision. Primary job functions do not typically require exercising independent judgment.

IT Senior INFOSEC Engineer
Education: B.A. or B.S. degree
Minimum Experience: Must possess a minimum of 10 years' experience.
Specialized Knowledge: Assessment and Authorization specialists advise and assist the Sponsor's customers with the Lifecycle Certification and Accreditation (C&A) process and developing a Systems Security Plan (SSP). Acts as C&A/A&A project register, managing the C&A process. Develop risk assessment reports: Based on review of SSP and interviews with developer/customer, assess systems against Intelligence Community Information Assurance policies and regulations, analyze risk, recommend mitigating countermeasures, and write short, succinct risk assessment and certification reports for submission to the Chief Information Officer and Executive Director. Assemble and submit C&A packages to Principal Accreditation Authority/Designated Accreditation Authority.
Cloud SME/Program Manager
Education: Master's degree or higher
Minimum Experience: Programming, Software Engineering, Cybersecurity or other related discipline from an accredited institution with more than 12 years relevant experience. Preferred to have a Cloud Certification.
Specialized Experience: Serves as a subject matter expert and oversees the development and implementation of cloud service architectures that leverage the capabilities of selected cloud providers and cloud-based solutions. Key Responsibilities include: Leads the integration of technologies to enable cross-organizational capabilities and services implementations, defines the architectures, cloud management tools, processes and standards and drive the establishment of cloud services, manages technologies including IaaS, SaaS, PaaS, Public/Hybrid/Community Cloud Service Provider offerings, cloud management tools, and converged infrastructure, oversees the establishment of project objectives, plans, schedules, and budgets and for managing the technical, operational, and financial performance of projects, manages other Cloud Architects and Cloud Administrators.
IT Senior Subject Matter Expert
Education: Master's degree (MS/MBA) or higher
Minimum Experience: Master's degree (MS/MBA) or higher and at least 10 years of information technology professional work experience; Programming, Engineering, Devsecops or other related discipline from an accredited institution with more than 10 years relevant experience.
Specialized Experience: This position requires at least 10 years' experience in information systems implementation, technical and functional design, development, configuration, or analysis of specific product or programmatic functions. Provides technical and managerial expert consultative support to a functional are of the project. Provide extremely high-level functional system development or analysis. Position incorporates the design, integration, documentation, implementation, and analysis on complex problems requiring knowledge of the technical subject matter. Makes recommendations and advises on organizational-wide systems improvements, optimization or maintenance efforts for a technical functional area which may include: Cloud Computing, Mobility, Distributed Systems Development, Web, Intranet, Warehousing, E- Commerce, Client-Server Development, Database Design and Development, Integration Services, IT Strategic Planning, Systems Analysis and Needs Assessment, and Business Process Reengineering. The IT Senior Subject Matter Expert I, based on experience and expertise may be involved in any or all stages of a project to include consulting, design, development, implementation, operation and/or training.

SIN 54151HACS

<p>Senior Penetration Tester</p>
<p>Education: Bachelor’s Degree in Computer Science, Programming, Software Engineering, or other related discipline from an accredited institution.</p>
<p>Minimum Experience: More than 10 years relevant experience. Must have at least four years of practical experience conducting penetration testing. Serve as the lead Penetration Tester and responsible for management of penetration testing program. Must have a working knowledge of NIST 800 series guidance for cyber security.</p>
<p>Specialized Knowledge: Conducts remote and onsite testing of Information Technology Systems (IT) to detect weaknesses, vulnerabilities, and compliance issues. Experienced in Network architectures, operating systems, application software, and cyber security tools and techniques. Expert in the use of penetration testing tools, techniques, and attack vectors to be used in a sanctioned attack or intrusion for the sole purpose of evaluating the security of an IT system and to discover weaknesses, vulnerabilities, or compliance issues that are unknown to the system owner.</p>
<p>Mid-Level Penetration Tester</p>
<p>Education: B.S. Degree in Computer Science, Programming, Software Engineering, or other related discipline from an accredited institution</p>
<p>Minimum Experience: More than 5 years relevant experience. Must have at least four years of practical experience conducting penetration testing. Must have a working knowledge of NIST 800 series guidance for cyber security.</p>
<p>Specialized Knowledge: Conducts remote and onsite testing of Information Technology Systems (IT) to detect weaknesses, vulnerabilities, and compliance issues. Experienced in Network architectures, operating systems, application software, and cyber security tools and techniques. Expert in the use of penetration testing tools, techniques, and attack vectors to be used in a sanctioned attack or intrusion for the sole purpose of evaluating the security of an IT system and to discover weaknesses, vulnerabilities, or compliance issues that are unknown to the system owner.</p>
<p>Senior Risk & Vulnerability Analyst</p>
<p>Education: B.S. Degree in Computer Science, Programming, Software Engineering, or other related discipline from an accredited institution</p>
<p>Minimum Experience: More than 8 years relevant experience. Experience in computer network defense and in-depth technical knowledge/mastery with intrusion detection systems. Must have a working knowledge of NIST 800 series guidance for cyber security.</p>
<p>Windows, Linux Operating Systems; Database security, Active Directory, Service Oriented Architectures, vulnerability testing, networking protocols and topologies, security architectures, and incident management. Develops technical solutions including: information operations and analysis related to security intrusion analysis, systems and vulnerabilities, network security, advanced analytic tools, data visualization techniques. Serves as lead analyst in the detection of malicious activity to prevent, detect, contain, and eradicated intrusions and intrusion attempts. Conduct analysis of system logs, forensic results, vulnerability assessment tool results, risk, and investigate instances of security concern throughout the enterprise. Ensure required cyber security policies are adhered to and that required controls are implemented.</p>

<p>Mid-Level Risk & Vulnerability Analyst</p>
<p>Education: B.S. Degree in Computer Science, Programming, Software Engineering, or other related discipline from an accredited institution</p>
<p>Minimum Experience: More than 5 years relevant experience. Experience in computer network defense and in-depth technical knowledge/mastery with intrusion detection systems. Must have a working knowledge of NIST 800 series guidance for cyber security.</p>
<p>Specialized Knowledge: Possess a working knowledge of network technologies such as: Windows, Linux Operating Systems; Database security, Active Directory, Service Oriented Architectures, vulnerability testing, networking protocols and topologies, security architectures, and incident management. Develops technical solutions including: information operations and analysis related to security intrusion analysis, systems and vulnerabilities, network security, advanced analytic tools, data visualization techniques. Serves as lead analyst in the detection of malicious activity to prevent, detect, contain, and eradicate intrusions and intrusion attempts. Ensure required cyber security policies are adhered to and that required controls are implemented. Experience Conducting Web application, operating system, database & wireless testing and assessments using COTS tools.</p>
<p>Senior Incident Response Analyst</p>
<p>Education: Bachelor's or Master's Degree in Computer Science or related discipline. 6 years of general experience is considered equivalent to a Bachelor's Degree.</p>
<p>Minimum Experience: More than 8 years of practical experience with incident response. Must have a working knowledge of NIST 800 series guidance for cyber security.</p>
<p>Specialized Knowledge: Under general direction, leads security event monitoring and correlation within a tiered Security Operations Center. Proven experience and ability to leverage CND analyst toolsets to detect and respond to IT security incidents. Ability to implement standard procedures for incident response interfacing with Information Security Officer and IT staff. Conducts research and document threats and their behavior to include monitoring external CSIRTS/CERTs. Provide recommendations to threat mitigation strategies. Employ effective web, email, and telephonic communications to clearly manage security incident response procedures. Perform routine event reporting over time including trend reporting and analysis. Experience required in security or network technology (Unix/Windows OS, Cisco/Juniper Routing-Switching) within a hands-on design/Implementation/Administration role. Demonstrates in-depth knowledge of TCP-IP protocol implementations for all common network services in addition to demonstrated capability to perform network packet analysis and anomaly detection. Professionally certified, within a CND discipline, as Technical Level III as defined by DODI 8570 is a requirement.</p>
<p>Mid-Level Incident Response Analyst</p>
<p>Education: Bachelor's or Master's Degree in Computer Science or related discipline. 6 years of general experience is considered equivalent to a Bachelor's Degree.</p>
<p>Minimum Experience: More than four years of practical experience with incident response. Must have a working knowledge of NIST 800 series guidance for cyber security.</p>
<p>Specialized Knowledge: Under general supervision, participates in security event monitoring and correlation within a tiered Security Operations Center. Proven experience and ability to leverage CND analyst toolsets to detect and respond to IT security incidents. Conducts research and document threats and their behavior to include monitoring external CSIRTS/CERTs. Assist in providing recommendations to threat mitigation strategies. Employ effective web, email, and telephonic communications to clearly manage security incident response procedures. Perform routine event reporting over time including trend</p>

reporting and analysis. Experience required in security or network technology (Unix/Windows OS, Cisco/Juniper Routing-Switching) within a hands-on Implementation or Administration role. Demonstrates thorough knowledge of TCP-IP protocol implementations for all common network services in addition to demonstrated capability to perform network packet analysis and anomaly detection. Professionally certified, within a CND discipline, as Technical Level II as defined by DODI 8570 is a requirement.

Cyber Subject Matter Authority

Education: Master's degree or higher

Minimum Experience: Programming, Software Engineering, Cybersecurity or other related discipline from an accredited institution with more than 16 years relevant experience. Prefer industry specific cyber certifications.

Specialized Knowledge: Recognized as an authority in a given domain of Cyber security, or proficient in highly demanded emergent cyber tools or processes required under special circumstances Duties may include:

- Apply subject matter authority to a specific incident, security application or enterprise environment to improve security posture or resolve organizational issues
- Generate issue papers and reporting
- Advise senior leadership on security issues

Senior Cyber Security Engineer

Education: Bachelor's degree or higher

Minimum Experience: Programming, Software Engineering, Cybersecurity or other related discipline from an accredited institution with more than 10 years relevant experience. Prefer industry specific cyber certifications.

Specialized Knowledge: Participate in special projects or investigations into specific technology or solution issues and research and piloting of new technologies. Serve as a point of contact for engineering efforts while maintaining compliance with the customer's policies and guidelines Duties may include:

- Configure and maintain policies
- Maintain documentation for exceptions to standards
- Provides timely and adequate response to threats/alerts
- Assess security events to drive to a resolution
- Provides timely and sufficient response to security incidents and assessment services
- Promotes security awareness

Senior Cyber Hunt Analyst

Education: Bachelor's or Master's Degree in Computer Science or related discipline

Minimum Experience: 8 years of general experience in Information Assurance, Information Security, or Forensics technical guidance and leadership. CISSP, or equivalent certification.

Specialized Knowledge: Under general direction, leads Provides leadership, technical supervision, and mentorship to forensics analysts. Plans, organizes, directs and conducts forensic analysis and intrusion investigations on a variety of electronic media. Documents computer network exploitation and defense techniques. Identifies, deters, monitors, and investigates computer and network intrusions. Manages digital forensics examinations through the entire lifecycle of an investigation. Conducts forensics analysis to support malicious software, cyber security incidents, system intrusion, or other (civil, criminal, or internal) investigations. Acquires, collects, documents, and preserves evidence from various forms of electronic media and equipment. Conducts detailed forensically sound investigation of computer storage media, network servers, live systems, and mobile devices to identify and document relevant findings. Develops high quality oral and written work product and presents complex technical matters clearly and concisely. Produces expert reports that withstands legal

scrutiny of opposing counsels. Provides technical guidance and assistance to legal staff while preventing of spoliation of evidence.
Mid-level Cyber Hunt Analyst
Education: Bachelor's Degree in Computer Science or related discipline
Minimum Experience: 4 years of experience in Information Assurance, Security, or Forensics. CISSP, or equivalent certification.
Specialized Knowledge: Under general supervision, Ability to work independently with minimal technical oversight. Plans, organizes, directs and conducts forensic analysis and intrusion investigations on a variety of electronic media. Documents computer network exploitation and defense techniques. Identifies, deters, monitors, and investigates computer and network intrusions. Manages digital forensics examinations through the entire lifecycle of an investigation. Conducts forensics analysis to support malicious software, cyber security incidents, system intrusion, or other (civil, criminal, or internal) investigations. Acquires, collects, documents, and preserves evidence from various forms of electronic media and equipment. Conducts detailed forensically sound investigation of computer storage media, network servers, live systems, and mobile devices to identify and document relevant findings. Develops high quality oral and written work product and presents complex technical matters clearly and concisely. Produces expert reports that withstand legal scrutiny of opposing counsel. Provides technical guidance and assistance to legal staff.

SIN 518210ERM

Data Entry Supervisor
Minimum 2 years' experience in data entry and database systems. Formal training in advanced word processing systems. Proficient in spreadsheets and/or graphics packages. BA/BS educational level.
Quality Assurance Specialist
Minimum of 3 years of experience in developing and implementing quality control methodologies to ensure compliance with quality assurance standards, guidelines and procedures. Develops and defines major and minor characteristics of quality including quality metrics. Conducts and/or participates in formal and informal reviews at pre-determined points through the development or project life cycle. BA/BS educational level.
Records Manager I
Minimum 1 year of experience in Records Disposition and Records Management Regulations. Experience in all phases of disposition per Federal regulations and guideline, including maintaining and scheduling records, retiring records to the Washington National Records Center and transferring records to the National Archives. Experience in records review, records inventories, developing vital records schedules, and evaluation of existing records management procedures. BA/BS educational level.
Records Manager II
Minimum 3 years' experience in Records Disposition and Records Management Regulations. Experience in all phases of disposition per Federal regulations and guideline, including maintaining and scheduling records, retiring records to the Washington National Records Center and transferring records to the National Archives. Experience in records review, records inventories, developing vital records schedules, and evaluation of existing records management procedures. BA/BS educational level.
Records Manager III
Minimum 5 years in all phases of life cycle records management. Experience in Records Disposition and Records Management Regulations. Experience in all phases of disposition per Federal regulations and guideline, including maintaining and scheduling records, retiring

<p>records to the Washington National Records Center and transferring records to the National Archives. Experience in records review, records inventories, developing vital records schedules, and evaluation of existing records management procedures. BA/BS educational level.</p>
<p>Records Management Associate</p>
<p>Minimum 3 years' experience in records inventories, files segregation and reorganization, records disposition, word processing and database management usage, including physical review and movement of files. Formal training by NARA. BA/BS educational level.</p>
<p>Records Clerk</p>
<p>Minimum 1 year records clerk and/or data entry experience related to records management. Completion of basic NARA course(s) in records management. Ability to lift and handle 40-pound boxes.</p>
<p>Records Management Consultant</p>
<p>Minimum of 3 years' experience is required, of which one year must be specialized. Specialized experience includes administration of UNIX or other open systems-compliant multi-user system, and current DBMS technologies. Performs system installation and integration of computer operating system software, network software, application software, computer hardware, and supporting network or telecommunications systems. General experience includes administration of multi-user computer systems and databases. BA/BS educational level.</p>
<p>Subject Matter Expert I</p>
<p>The SME has 10 years' experience providing specific subject matter expertise and has a BA/BS educational level. Analyzes user needs to determine functional requirements. Performs functional allocation to identify required tasks and their interrelationships. Possesses requisite knowledge and expertise to be recognized in the professional community such that the Government is able to qualify the individual as an expert in design, engineering, finance, energy, outreach, or acquisition. Demonstrates exceptional oral and written communication skills.</p>
<p>Subject Matter Expert II</p>
<p>The SME has 15 years' experience providing specific subject matter expertise and has a BA/BS educational level. Analyzes user needs to determine functional requirements. Performs functional allocation to identify required tasks and their interrelationships. Possesses requisite knowledge and expertise to be recognized in the professional community such that the Government is able to qualify the individual as an expert in design, engineering, finance, energy, outreach, or acquisition. Demonstrates exceptional oral and written communication skills.</p>