## GSA AUTHORIZED FEDERAL SUPPLY SERVICE

## MULTIPLE AWARD SCHEDULE (MAS) PRICELIST

# Easy Dynamics Corporation

2000 Corporate Ridge, Suite 240
McLean, VA 22102
Phone: (202) 558-7275
Fax: (800) 466-0519
www.easydynamics.com
**SBA Certified 8(a) Woman Owned Small Business**

Contract Number: GS-35F-234BA
Period Covered by Contract: 2/20/2019 – 2/19/2024

Pricelist current through MAS Refresh #14 and Modification PS-A847 dated 7/5/2022.

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

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

## General Purpose Commercial Information Technology Equipment, Software and Services - FSC Group 70

| | |
|---|---|
| Special Item No. 54151S | Information Technology Professional Services |
| Special Item No. 54151SSTLOC | Information Technology Professional Services |
| Special Item No. 518210C | Cloud Related Professional Services |
| Special Item No. 518210CSTLOC | Cloud Related Professional Services |
| Special Item No. 541519ICAM | Identity, Credentialing & Access Management |
| Special Item No. 541519ICAMSTLOC | Identity, Credentialing & Access Management |
| Special Item No. 54151HACS | Highly Adaptive Cybersecurity Services |
| Special Item No. 54151HACSSTLOC | Highly Adaptive Cybersecurity Services |
| Special Item No. OLM | Order Level Materials |

| | |
|---|---|
| **SIN 54151S** | **Information Technology Professional Services** |
| FSC/PSC Code DA01 | IT and Telecom - Other Information Technology Services |
| **SIN 518210C** | **Cloud and Cloud-Related IT Professional** |
| FSC/PSC Code DB10 | IT and Telecom Cloud Computing Services |
| **SIN 541519ICAM** | **Identity, Credentialing & Access Management** |
| FSC/PSC Code DJ01 | IT and Telecom - Other Information Technology Services |
| **SIN 54151HACS** | **Highly Adaptive Cybersecurity Services** |
| FSC/PSC Code DJ01 | IT and Telecom - Other Information Technology Services |

## CUSTOMER INFORMATION:

**1a. Awarded Special Item Number(s):**

| SIN | Description |
|---|---|
| **518210C** | **Cloud-Related IT Professional Services** |
| **518210CSTLOC** | **Cloud-Related IT Professional Services** |
| **54151S** | **Information Technology Services** |
| **54151SSTLOC** | **Information Technology Services** |
| **541519ICAM** | **Identity, Credentialing and Access Management Services** |
| **541519ICAMSTLOC** | **Identity, Credentialing and Access Management Services** |
| **54151HACS** | **Highly Adaptive Cybersecurity Services** |
| **54151HACSSTLOC** | **Highly Adaptive Cybersecurity Services** |
| **OLM** | **Order-Level Materials (OLMs)** |

**1b**. Identification of the lowest priced labor category description, job title # and hourly rate awarded under the contract is:

| Job Title # | Labor Category Description | GSA Hourly Rate |
|---|---|---|
| Functional Systems Analyst I | Responsible for the technical implementation of the assigned system, across company's projects, according to the relevant customer's specification and the current requirements. Works with Product management to define requirements; works with engineering to define the high-level design for a real time system; ensures designs achieve high availability, maintainability and reliability of the product; helps define the future system architecture leading to increased capacity and availability. | $91.63 |

**1c**. Labor Category Descriptions of all corresponding commercial job titles, experience, functional responsibility and education are outlined on pages 13-18 within this pricelist.

**2. Maximum Order Threhold:** $500,000 – SIN 518210C, SIN 54151S, SIN 54141HACS; $1,000,000 – SIN 541519ICAM.

**3. Minimum Order:** $100

**4. Geographic Scope of Coverage:** The Geographic Scope of Coverage is Domestic Delivery. This is delivery within the 48 contiguous states, Alaska, Hawaii, Puerto Rico, Washington, DC, and U.S. Territories. Domestic delivery also includes a port or consolidation point, within the aforementioned areas, for orders received from overseas activities.

**5. Point(s) of production (city, county, and State or foreign country):** Not applicable

**6. Discount from list prices or statement of net price:** Net prices set forth below**.**

**7. Quantity Discount:** None

**8. Prompt Payment Terms:** None

**9a. Government purchase cards:** Accepted at or below the micro-purchase threshold.

**9b**. **Government purchase cards:** Accepted above the micro-purchase threshold.

**10. Foreign Items:** No foreign items are awarded under this contract.

**11a. Time of Delivery** – 30 Days

**11b. Expedited Delivery Terms:** As negotiated between Easy Dynamics and the Ordering Activity

**11c. Overnight/2-Day Delivery Terms:** As negotiated between Easy Dynamics and the Ordering Activity

**11d. Urgent Requirements:** When the Federal Supply Schedule contract delivery period does not meet the bona fide urgent delivery requirements of an ordering activity, ordering activities are encouraged, if time permits, to contact the Contractor for the purpose of obtaining accelerated delivery. The Contractor shall reply to the inquiry within 3 workdays after receipt. (Telephonic replies shall be confirmed by the Contractor in writing.) If the Contractor offers an accelerated delivery time acceptable to the ordering activity, any order(s) placed pursuant to the agreed upon accelerated delivery time frame shall be delivered within this shorter delivery time and in accordance with all other terms and conditions of the contract.

**12. FOB Point:** Destination

**13a. Ordering Address:**
2000 Corporate Ridge
Suite 240
McLean, VA 22102
Attn: contracts@easydynamics.com

**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:**
2000 Corporate Ridge
Suite 240
McLean, VA 22102
Attn: AccountsPayable@easydynamics.com

**15. Warranty/Guarantee Provisions:** All services performed under this contract will be guaranteed to completed in a satisfactory workmanlike manner as delineated with this Authorized FSS IT Schedule Pricelist.

**16. Export Packing Charges:** Export Packing is not offered under this contract.

**17. Terms and conditions of Government purchase card acceptance (any thresholds above the micro-purchase level).** – Purchase cards accepted

**18. Terms and conditions of rental, maintenance, and repair**– Not Applicable

**19. Terms and conditions of installation** – Not Applicable

**20. Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices** – Not Applicable

**20a**. **Terms and conditions for any other services** – Not Applicable

**21. List of service and distribution points:** Not Applicable

**22. List of Participating Dealers:** Easy Dynamics does not authorize any participating dealers under this contract.

**23. Preventive maintenance –** Not Applicable

**24a. Environmental Attributes (**e.g., recycled content, energy efficiency, and/or reduced pollutants): Not Applicable

**24b. Section 508 Compliance**: Contact Easy Dynamics for Section 508 compliance information. The EIT standards can be found at: http://www.section508.gov

**25. Data Universal Numbering System (DUNS) Number:** 805890832

**Unique Entity Identifier:** T2GJTLGN2NP3

**Taxpayer Idenfication Number** (TIN): N/A

**Business Size**: SBA Certified 8(a) Women Owned Small Businesses

**CAGE Code:** 57QD0

**26. Notification regarding registration in Central Contractor Registration (CCR) database:** Easy Dynamics Corporation is currently registered within the System for Award Management (SAM) database.

**27. Trade Agreements Act of 1979, as Amended:** All items are U.S. made end products, designated country end products, Caribbean Basin country end products, Canadian end products, or Mexican end products as defined in the Trade Agreements Act of 1979, as amended.

**28. Ordering Procedures for Federal Supply Schedule Contracts:** Ordering activities shall use the ordering procedures of Federal Acquisition Regulation (FAR) 8.405 when placing an order or establishing a BPA for supplies or serJvices. These procedures apply to all schedules.

a. FAR 8.405-1 Ordering procedures for supplies, and services not requiring a statement of work.

b. FAR 8.405-2 Ordering procedures for services requiring a statement of work.

**29. Contractor Tasks/Special Requirements (C-FSS-370) (NOV 2003):**

(a) Security Clearances: The Contractor may be required to obtain/possess varying levels of security clearances in the performance of orders issued under this contract. All costs associated with obtaining/possessing such security clearances should be factored into the price offered under the Multiple Award Schedule.

(b) Travel: The Contractor may be required to travel in performance of orders issued under this contract. Allowable travel and per diem charges are governed by Pub .L. 99-234 and FAR Part 31, and are reimbursable by the ordering agency or can be priced as a fixed price item on orders placed under the Multiple Award Schedule. Travel in performance of a task order will only be reimbursable to the extent authorized by the ordering agency. The Industrial Funding Fee does NOT apply to travel and per diem charges.

(c) Certifications, Licenses and Accreditations: As a commercial practice, the Contractor may be required to obtain/possess any variety of certifications, licenses and accreditations for specific FSC/service code classifications offered. All costs associated with obtaining/ possessing such certifications, licenses and accreditations should be factored into the price offered under the Multiple Award Schedule program.

(d) Insurance: As a commercial practice, the Contractor may be required to obtain/possess insurance coverage for specific FSC/service code classifications offered. All costs associated with obtaining/possessing such insurance should be factored into the price offered under the Multiple Award Schedule program.

(e) Personnel: The Contractor may be required to provide key personnel, resumes or skill category descriptions in the performance of orders issued under this contract. Ordering activities may require agency approval of additions or replacements to key personnel.

(f) Organizational Conflicts of Interest: Where there may be an organizational conflict of interest as determined by the ordering agency, the Contractor’s participation in such order may be restricted in accordance with FAR Part 9.5.

(g) Documentation/Standards: The Contractor may be requested to provide products or services in accordance with rules, regulations, OMB orders, standards and documentation as specified by the agency’s order.

(h) Data/Deliverable Requirements: Any required data/deliverables at the ordering level will be as specified or negotiated in the agency’s order.

(i) Government-Furnished Property: As specified by the agency’s order, the Government may provide property, equipment, materials or resources as necessary.

(j) Availability of Funds: Many Government agencies’ operating funds are appropriated for a specific fiscal year. Funds may not be presently available for any orders placed under the contract or any option year. The Government’s obligation on orders placed under this contract is contingent upon the availability of appropriated funds from which payment for ordering purposes can be made. No legal liability on the part of the Government for any payment may arise until funds are available to the ordering Contracting Officer.

(k) Overtime: For professional services, the labor rates in the Schedule should not vary by virtue of the Contractor having worked overtime. For services applicable to the Service Contract Act (as identified in the Schedule), the labor rates in the Schedule will vary as governed by labor laws (usually assessed a time and a half of the labor rate).

**30. Contract Administration for Ordering Activities:** Any ordering activity, with respect to any one or more delivery orders placed by it under this contract, may exercise the same rights of termination as might the GSA Contracting Officer under provisions of FAR 52.212-4, paragraphs (l) Termination for the ordering activity's convenience, and (m) Termination for Cause (See 52.212-4)

**31. Contractor Commitments, Warranties and Representations:**

a. For the purpose of this contract, commitments, warranties and representations include, in addition to those agreed to for the entire schedule contract:

(1) Time of delivery/installation quotations for individual orders;

(2) Technical representations and/or warranties of products concerning performance, total system performance and/or configuration, physical, design and/or functional characteristics and capabilities of a product/equipment/ service/software package submitted in response to requirements which result in orders under this schedule contract.

(3) Any representations and/or warranties concerning the products made in any literature, description, drawings and/or specifications furnished by the Contractor.

b. The above is not intended to encompass items not currently covered by the GSA Schedule contract.

**32. Blanket Purchase Agreements (BPAs): T**he use of BPAs under any schedule contract to fill repetitive needs for supplies or services is allowable. BPAs may be established with one or more schedule contractors. The number of BPAs to be established is within the discretion of the ordering activity establishing the BPA and should be based on a strategy that is expected to maximize the effectiveness of the BPA(s). Ordering activities shall follow FAR 8.405-3 when creating and implementing BPA(s).

**33. Contractor Team Arrangements:** Contractors participating in contractor team arrangements must abide by all terms and conditions of their respective contracts. This includes compliance with Clauses 552.238-74, Industrial Funding Fee and Sales Reporting, i.e., each contractor (team member) must report sales and remit the IFF for all products and services provided under its individual contract.

**34. Installation, Deinstallation, Reinstallation:** The Davis-Bacon Act (40 U.S.C. 276a-276a-7) provides that contracts in excess of $2,000 to which the United States or the District of Columbia is a party for construction, alteration, or repair (including painting and decorating) of public buildings or public works with the United States, shall contain a clause that no laborer or mechanic employed directly upon the site of the work shall received less than the prevailing wage rates as determined by the Secretary of Labor. The requirements of the Davis-Bacon Act do not apply if the construction work is incidental to the furnishing of supplies, equipment, or services. For example, the requirements do not apply to simple installation or alteration of a public building or public work that is incidental to furnishing supplies or equipment under a supply contract. However, if the construction, alteration or repair is segregable and exceeds $2,000, then the requirements of the Davis-Bacon Act applies.

The ordering activity issuing the task order against this contract will be responsible for proper administration and enforcement of the Federal labor standards covered by the Davis-Bacon Act. The proper Davis-Bacon wage determination will be issued by the ordering activity at the time a request for quotations is made for applicable construction classified installation, deinstallation, and reinstallation services under SIN 33411 or 33411REF.

**35. Prime Contractor Ordering from Federal Supply Schedules:** Prime Contractors (on cost reimbursement contracts) placing orders under Federal Supply Schedules, on behalf of an ordering activity, shall follow the terms of the applicable schedule and authorization and include with each order

(a) A copy of the authorization from the ordering activity with whom the contractor has the prime contract (unless a copy was previously furnished to the Federal Supply Schedule contractor); and

(b) The following statement:

> This order is placed under written authorization from _______ dated _______. In the event of any inconsistency between the terms and conditions of this order and those of your Federal Supply Schedule contract, the latter will govern.

**36. Insurance- Work On A Government Installation (JAN 1997)(FAR 52.228-5):**

(a) The Contractor shall, at its own expense, provide and maintain during the entire performance of this contract, at least the kinds and minimum amounts of insurance required in the Schedule or elsewhere in the contract.

(b) Before commencing work under this contract, the Contractor shall notify the Contracting Officer in writing that the required insurance has been obtained. The policies evidencing required insurance shall contain an endorsement to the effect that any cancellation or any material change adversely affecting the Government's interest shall not be effective—

> (1) For such period as the laws of the State in which this contract is to be performed prescribe; or
>
> (2) Until 30 days after the insurer or the Contractor gives written notice to the Contracting Officer, whichever period is longer.

(c) The Contractor shall insert the substance of this clause, including this paragraph (c), in subcontracts under this contract that require work on a Government installation and shall require subcontractors to provide and maintain the insurance required in the Schedule or elsewhere in the contract. The Contractor shall maintain a copy of all subcontractors' proofs of required insurance, and shall make copies available to the Contracting Officer upon request.

**37. Advance Payments:** A payment under this contract to provide a service or deliver an article for the United States Government may not be more than the value of the service already provided or the article already delivered. Advance or pre-payment is not authorized or allowed under this contract. (31 U.S.C. 3324)

## TERMS AND CONDITIONS APPLICABLE TO PURCHASE OF CLOUD COMPUTING PRODUCTS AND CLOUD RELATED IT PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 518210C)

****NOTE: This SIN presents a solution for Contractors to provide cloud computing services and cloud-related IT professional services that comply with NIST definitions and principles within the scope of today’s technology and standards with a secondary goal of accommodating ongoing technical advances in cloud computing. SIN 518210 Cloud Computing Services and Cloud-Related IT Professional Services is designed to cover core Cloud Services including Infrastructure as a Service, Platform as a Service, and Software as a Service, as well as the Cloud-related IT Professional Services required to assess, prepare, refactor, migrate, DevOps, integrate or govern a Cloud implementation.

In accordance with section 889 of the National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232, August 13, 2018), an executive agency will be prohibited one year after enactment of the Act from procuring, obtaining, extending or renewing a contract to procure or obtain any equipment, system or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system; and two years after enactment of the Act from entering into, renewing or extending a contract with an entity that uses covered telecommunications equipment or service in that entity's equipment, system or service, as a substantial or essential component of any system, or as critical technology as part of any system. Section 889 defines "covered telecommunications equipment or services" as any of the following:

(A) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities).

(B) For the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities).

(C) Telecommunications or video surveillance services provided by such entities or using such equipment.

(D) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or **controlled** by, or otherwise connected to, the government of a covered foreign country (i.e. the People's Republic of China). (Pub. L. 115-232, section 889(f)(3), italicized parenthetical added).

**1. SCOPE**

The prices, terms and conditions stated under Special Item Number (SIN) 518210C Cloud Computing Services (i.e. IaaS, etc.) and Cloud-Related Professional Services apply exclusively to Cloud Computing Services (i.e. IaaS, etc.) and Cloud-Related Professional Services within the scope of this Information Technology Schedule.

This SIN provides ordering activities with access to Cloud (i.e. SaaS, etc.) technical services that run in cloud environments and meet the NIST Definition of Cloud Computing Essential Characteristics. Cloud Services [(i.e. SaaS, etc.)] relating to or impinging on cloud that do not meet all NIST essential characteristics should be listed in other SINs. (For example: Software subscription services or Software as a Service offerings that do not meet the essential "measured service" requirement may meet the definition of "Term Licenses" under SIN 511210. See the Measured Service requirement in Table 2, below.)

The scope of this SIN is limited to cloud capabilities provided entirely as a "pay as you go" service and cloud-related IT professional services. Hardware, software and other artifacts acquired to supporting the physical construction of a private or other cloud are out of scope for this SIN. Currently, an Ordering Activity can procure the hardware and software needed to build private on premise cloud functionality, through combining different services on other GSA Schedule SINs (e.g. 33411, 511210, 54151, 54151ECOM, 54151S).

Sub-categories in scope for this SIN are the three NIST Service Models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Offerors may optionally select a single sub-category that best fits a proposed cloud service offering. Only one sub-category may be selected per each proposed cloud service offering. Offerors may elect to submit multiple cloud service offerings, each with its own single sub-category. The selection of one of three sub-categories does not prevent Offerors from competing for orders under the other two sub-categories.

See service model guidance for advice on sub-category selection.

Sub-category selection within this SIN is optional for any individual cloud service offering, and new cloud computing service (i.e. IaaS, etc.) technologies that do not align with the aforementioned three sub-categories may be included without a sub-category selection so long as they comply with the essential characteristics of cloud computing as outlined by NIST. See Table 1 for a representation of the scope and sub-categories.

**Table 1: Cloud Computing Services (i.e. IaaS, etc.)**

| **SIN Description** | **Sub-Categories**[1] |
|---|---|
| ● Commercially available cloud computing services<br>● Meets the National Institute for Standards and Technology (NIST) definition of Cloud Computing essential characteristics<br>● Open to all deployment models (private, public, community or hybrid), vendors specify deployment models | **1. Software as a Service (SaaS):** Consumer uses provider's applications on cloud infrastructure. Does not manage/control platform or infrastructure. Limited application level configuration may be available.<br>**2. Platform as a Service (PaaS):** Consumer deploys applications onto cloud platform service using provider-supplied tools. Has control over deployed applications and some limited platform configuration but does not manage the platform or infrastructure.<br>**3. Infrastructure as a Service (IaaS):** Consumer provisions computing resources. Has control over OS, storage, platform, deployed applications and some limited infrastructure configuration, but does not manage the infrastructure. |

## 2. RESERVED

## 3. RESPONSIBILITIES OF THE CONTRACTOR

The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character.

### a. Acceptance Testing

Any required Acceptance Test Plans and Procedures shall be negotiated by the Ordering Activity at task order level. The Contractor shall perform acceptance testing of the systems for Ordering Activity approval in accordance with the approved test procedures.

### b. Training

[1] Offerors may optionally select the single sub-category that best fits each cloud service offering, per Service Model Guidance, or select no sub-category if the offering does not fit an existing NIST service model.

If training is provided commercially the Contractor shall provide normal commercial installation, operation, maintenance, and engineering interface training on the system. Contractor is responsible for indicating if there are separate training charges.

### c. Information Assurance/Security Requirements

The contractor shall meet information assurance/security requirements in accordance with the Ordering Activity requirements at the Task Order level.

### d. Related Professional Services

The Contractor is responsible for working with the Ordering Activity to identify related professional services and any other services available on other SINs that may be associated with deploying a complete cloud service (i.e. IaaS, etc.) solution. Any additional substantial and ongoing IT professional services related to the offering such as assessing, preparing, refactoring, migrating, DevOps, developing new cloud based applications and managing/governing a cloud implementation may be offered per the guidelines below.

### e. Performance of Cloud Computing Services (i.e. IaaS, etc.)

The Contractor shall respond to Ordering Activity requirements at the Task Order level with proposed capabilities to Ordering Activity performance specifications or indicate that only standard specifications are offered. In all cases the Contractor shall clearly indicate standard service levels, performance and scale capabilities.

The Contractor shall provide appropriate cloud computing services (i.e. IaaS, etc.) on the date and to the extent and scope agreed to by the Contractor and the Ordering Activity.

### f. Reporting

The Contractor shall respond to Ordering Activity requirements and specify general reporting capabilities available for the Ordering Activity to verify performance, cost and availability.

In accordance with commercial practices, the Contractor may furnish the Ordering Activity/user with a monthly summary Ordering Activity report.

## 4. RESPONSIBILITIES OF THE ORDERING ACTIVITY

The Ordering Activity is responsible for indicating the cloud computing services requirements unique to the Ordering Activity. Additional requirements should not contradict existing SIN or GSA Schedule Terms and Conditions. Ordering Activities should include (as applicable) Terms & Conditions to address Pricing, Security, Data Ownership, Geographic Restrictions, Privacy, SLAs, etc.

Cloud services typically operate under a shared responsibility model, with some responsibilities assigned to the Cloud Service Provider (CSP), some assigned to the Ordering Activity, and others shared between the two. The distribution of responsibilities will vary between providers and across service models. Ordering activities should engage with CSPs to fully understand and evaluate the shared responsibility model proposed. Federal Risk and Authorization Management Program (FedRAMP) documentation will be helpful regarding the security aspects of shared responsibilities, but operational aspects may require additional discussion with the provider.

### a. Ordering Activity Information Assurance/Security Requirements Guidance

(1) The Ordering Activity is responsible for ensuring to the maximum extent practicable that each requirement issued is in compliance with the Federal Information Security Management Act (FISMA) as applicable.

(2) The Ordering Activity shall assign a required impact level for confidentiality, integrity and availability (CIA) prior to issuing the initial statement of work.[2] The Contractor must be capable of meeting at least the minimum security requirements assigned against a low-impact information system in each CIA assessment area (per FIPS 200) and must detail the FISMA capabilities of the system in each of CIA assessment area.

(3) Agency level FISMA certification, accreditation, and evaluation activities are the responsibility of the Ordering Activity. The Ordering Activity reserves the right to independently evaluate, audit, and verify the FISMA compliance for any proposed or awarded Cloud Computing Services.

(4) The Ordering Activity has final responsibility for assessing the FedRAMP status of the service, complying with and making a risk-based decision to grant an Authorization to Operate (ATO) for the cloud computing service, and continuous monitoring. A memorandum issued by the Office of Management and Budget (OMB) on Dec 8, 2011 outlines the responsibilities of Executive departments and agencies in the context of FedRAMP compliance.[3]

(5) Ordering activities are responsible for determining any additional information assurance and security related requirements based on the nature of the application and relevant mandates.

### b. Deployment Model

If a particular deployment model (Private, Public, Community, or Hybrid) is desired, Ordering Activities are responsible for identifying the desired model(s). Alternately, Ordering Activities could identify requirements and assess Contractor responses to determine the most appropriate deployment model(s).

### c. Delivery Schedule

The Ordering Activity shall specify the delivery schedule as part of the initial requirement. The Delivery Schedule options are found in Information for Ordering Activities Applicable to All Special Item Numbers.

### d. Interoperability

Ordering Activities are responsible for identifying interoperability requirements. Ordering Activities should clearly delineate requirements for API implementation and standards conformance.

### e. Performance of Cloud Computing Services

The Ordering Activity should clearly indicate any custom minimum service levels, performance and scale requirements as part of the initial requirement.

### f. Reporting

The Ordering Activity should clearly indicate any cost, performance or availability reporting as part of the initial requirement.

### g. Privacy

The Ordering Activity should specify the privacy characteristics of their service and engage with the Contractor to determine if the cloud service is capable of meeting Ordering Activity requirements. For

**[2] Per Federal Information Processing Standards Publication 199 & 200 (FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems") (FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems")**

[3] MEMORANDUM FOR CHIEF INFORMATION OFFICERS: Security Authorization of Information Systems in Cloud Computing Environments. December 8, 2011.

example, a requirement could be requiring assurance that the service is capable of safeguarding Personally Identifiable Information (PII), in accordance with NIST SP 800-122[4] and OMB memos M-06-16[5] and M-07-16[6]. An Ordering Activity will determine what data elements constitute PII according to OMB Policy, NIST Guidance and Ordering Activity policy.

### h. Accessibility

The Ordering Activity should specify the accessibility characteristics of their service and engage with the Contractor to determine the cloud service is capable of meeting Ordering Activity requirements. For example, a requirement could require assurance that the service is capable of providing accessibility based on Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d).

### i. Geographic Requirements

Ordering activities are responsible for specifying any geographic requirements and engaging with the Contractor to determine that the cloud services offered have the capabilities to meet geographic requirements for all anticipated task orders. Common geographic concerns could include whether service data, processes and related artifacts can be confined on request to the United States and its territories, or the continental United States (CONUS).

### j. Data Ownership and Retrieval and Intellectual Property

Intellectual property rights are not typically transferred in a cloud model. In general, CSPs retain ownership of the Intellectual Property (IP) underlying their services and the customer retains ownership of its intellectual property. The CSP gives the customer a license to use the cloud services (i.e. IaaS, etc.) for the duration of the contract without transferring rights. The government retains ownership of the IP and data they bring to the customized use of the service as spelled out in the FAR and related materials.

General considerations of data ownership and retrieval are covered under the terms of the GSA Schedule and the FAR and other laws, ordinances, and regulations (Federal, State, City, or otherwise). Because of considerations arising from cloud shared responsibility models, ordering activities should engage with the Contractor to develop more cloud-specific understandings of the boundaries between data owned by the government and that owned by the cloud service provider, and the specific terms of data retrieval.

In all cases, the Ordering Activity should enter into an agreement with a clear and enforceable understanding of the boundaries between government and cloud service provider data, and the form, format and mode of delivery for each kind of data belonging to the government.

The Ordering Activity should expect that the Contractor shall transfer data to the government at the government's request at any time, and in all cases when the service or order is terminated for any reason, by means, in formats and within a scope clearly understood at the initiation of the service. Example cases that might require clarification include status and mode of delivery for:

- Configuration information created by the government and affecting the government's use of the cloud provider's service.
- Virtual machine configurations created by the government but operating on the cloud provider's service.

[4] NIST SP 800-122, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)"

[5] OMB memo M-06-16: Protection of Sensitive Agency Information
http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf

[6] OMB Memo M-07-16: Safeguarding Against and Responding to the Breach of Personally Identifiable Information
http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf

- Profile, configuration and other metadata used to configure SaaS application services or PaaS platform services.

The key is to determine in advance the ownership of classes of data and the means by which Government owned data can be returned to the Government.

### k. Service Location Distribution

The Ordering Activity should determine requirements for continuity of operations and performance and engage with the Contractor to ensure that cloud services have adequate service location distribution to meet anticipated requirements. Typical concerns include ensuring that:

(1) Physical locations underlying the cloud are numerous enough to provide continuity of operations and geographically separate enough to avoid an anticipated single point of failure within the scope of anticipated emergency events.

(2) Service endpoints for the cloud are able to meet anticipated performance requirements in terms of geographic proximity to service requestors.

Note that cloud providers may address concerns in the form of minimum distance between service locations, general regions where service locations are available, etc.

## 5. GUIDANCE FOR CONTRACTORS

This section offers guidance for interpreting the Contractor Description Requirements in Table 2, including the NIST essential cloud characteristics, service models and deployment models. This section is not a list of requirements.

Contractor-specific definitions of cloud computing characteristics and models or significant variances from the NIST essential characteristics or models are discouraged and will not be considered in the scope of this SIN or accepted in response to Factors for Evaluation. The only applicable cloud characteristics, service model/subcategories and deployment models for this SIN will be drawn from the NIST 800-145 special publication. Services qualifying for listing as cloud computing services (i.e. IaaS, etc.) under this SIN must substantially satisfy the essential characteristics of cloud computing as documented in the NIST Definition of Cloud Computing SP 800-1457.

Contractors must select deployment models corresponding to each way the service can be deployed. Multiple deployment model designations for a single cloud service are permitted but at least one deployment model must be selected.

In addition, contractors submitting Cloud services (i.e. IaaS, etc.) for listing under this SIN are encouraged to select a sub-category for each Cloud service (i.e. IaaS, etc.) proposed under this SIN with respect to a single principal NIST cloud service model that most aptly characterizes the service. Cloud Service model (i.e. IaaS, etc.) categorization is optional.

## General Guidance

Both Cloud service model (i.e. IaaS, etc.) and deployment model (i.e. public, etc.) designations must accord with NIST definitions. Guidance is offered in this document on making the most appropriate selection

### a. NIST Essential Characteristics

NIST’s essential cloud characteristics provide a consistent metric for whether a service is eligible for inclusion in this SIN. It is understood that due to legislative, funding and other constraints that government entities cannot always leverage a cloud service to the extent that all NIST essential characteristics are commercially available. For the purposes of the Cloud SIN, meeting the NIST essential characteristics is determined by whether each essential capability of the commercial service is available for the service, whether or not the Ordering Activity actually requests or implements the capability. The guidance in Table 3 offers examples of how services might or might not be included based on the essential characteristics, and how the Contractor should interpret the characteristics in light of current government contracting processes.

**Table 3: Guidance on Meeting NIST Essential Characteristics**

| Characteristic | Capability | Guidance |
|---|---|---|
| On-Demand Self-Service | ● Ordering activities can directly provision services without requiring Contractor intervention.<br>● This characteristic is typically implemented via a service console or programming interface for provisioning | Government procurement guidance varies on how to implement on-demand provisioning at this time. Ordering activities may approach on-demand in a variety of ways, including "not-to-exceed" limits, or imposing monthly or other appropriate payment cycles on what are essentially on demand services.<br>Services under this SIN must be capable of true on- demand self-service, and ordering activities and Contractors must negotiate how they implement on demand capabilities in practice at the task order level:<br>● Ordering activities must specify their procurement approach and requirements for on-demand service<br>● Contractors must propose how they intend to meet the approach<br>● Contractors must certify that on-demand self-service is technically available for their service should procurement guidance become available. |
| Broad Network Access | ● Ordering activities are able to access services over standard agency networks.<br>● Service can be accessed and provisioned using standard devices such as browsers, tablets and mobile phones | ● Broad network access must be available without significant qualification and in relation to the deployment model and security domain of the services.<br>● Contractors must specify any ancillary activities, services or equipment required to access cloud services or integrate cloud with other cloud or non- cloud networks and services. For example, a private cloud might require an Ordering Activity to purchase or provide a dedicated router, etc. which is acceptable but should be indicated by the Contractor. |
| Resource Pooling | ● Pooling distinguishes cloud services from simple offsite hosting.<br>● Ordering activities draw resources from a common pool maintained by the Contractor<br>● Resources may have general characteristics such as regional location | ● The cloud service must draw from a pool of resources and provide an automated means for the Ordering Activity to dynamically allocate them.<br>●Manual allocation, e.g. manual operations at a physical server farm where Contractor staff configure servers in response to Ordering Activity requests, does not meet this requirement<br>● Similar concerns apply to software and platform models; automated provisioning from a pool is required<br>● Ordering activities may request dedicated physical hardware, software or platform resources to access a private cloud deployment service. However the provisioned cloud resources must be drawn from a common pool and automatically allocated on request. |

| | | |
|---|---|---|
| Measured Service | ● Measured service should be understood as a reporting requirement that enables an Ordering Activity to control their use in cooperation with self service | ● Procurement guidance for on-demand self-service applies to measured service as well, i.e. rapid elasticity must be technically available but ordering activities and Contractors may mutually designate other contractual arrangements.<br>● Regardless of specific contractual arrangements, reporting must indicate actual usage, be continuously available to the Ordering Activity, and provide meaningful metrics appropriate to the service measured<br>● Contractors must specify that measured service is available and the general sort of metrics and mechanisms available<br>● The goal of the Measured Service requirement is to ensure Ordering Activities realize the full benefit of “pay as you go” consumption models. Consumption measurements that are not discrete enough or frequent enough (greater than 30 days), will not fulfill this NIST essential characteristic and will not be eligible for inclusion in this SIN. |

### Inheriting Essential Characteristics

Cloud Services (i.e. IaaS, etc.) may depend on other cloud services, and cloud service models such as PaaS and SaaS are able to inherit essential characteristics from other cloud services that support them. For example a PaaS platform service can inherit the broad network access made available by the IaaS service it runs on, and in such a situation would be fully compliant with the broad network access essential characteristic. Cloud Services (i.e. IaaS, etc.) inheriting essential characteristics must make the inherited characteristic fully available at their level of delivery to claim the relevant characteristic by inheritance.

Inheriting characteristics does not require the inheriting provider to directly bundle or integrate the inherited service, but it does require a reasonable measure of support and identification. For example, the Ordering Activity may acquire an IaaS service from “Provider A” and a PaaS service from “Provider B”. The PaaS service may inherit broad network access from “Provider A” but must identify and support the inherited service as an acceptable IaaS provider.

### Assessing Broad Network Access

Typically broad network access for public deployment models implies high bandwidth access from the public internet for authorized users. In a private cloud deployment internet access might be considered broad access, as might be access through a dedicated shared high bandwidth network connection from the Ordering Activity, in accord with the private nature of the deployment model.

### Resource Pooling and Private Cloud

All cloud resource pools are finite, and only give the appearance of infinite resources when sufficiently large, as is sometimes the case with a public cloud. The resource pool supporting a private cloud is typically smaller with more visible limits. A finite pool of resources purchased as a private cloud service qualifies as resource pooling so long as the resources within the pool can be dynamically allocated to the ultimate users of the resource, even though the pool itself appears finite to the Ordering Activity that procures access to the pool as a source of dynamic service allocation.

**b. NIST Service Model**

The Contractor may optionally document the service model of cloud computing (e.g. IaaS, PaaS, SaaS, or a combination thereof, that most closely describes their offering, using the definitions in The NIST

Definition of Cloud Computing SP 800-145. The following guidance is offered for the proper selection of service models.

NIST's service models provide this SIN with a set of consistent sub-categories to assist ordering activities in locating and comparing Cloud services (i.e. IaaS, etc.) of interest. Service model is primarily concerned with the nature of the service offered and the staff and activities most likely to interact with the service. Contractors should select a single service model most closely corresponding to their proposed service based on the guidance below. It is understood that cloud services can technically incorporate multiple service models and the intent is to provide the single best categorization of the service.

Contractors should take care to select the NIST service model most closely corresponding to each service offered. Contractors should not invent, proliferate or select multiple cloud service model sub-categories to distinguish their offerings, because ad-hoc categorization prevents consumers from comparing similar offerings. Instead vendors should make full use of the existing NIST categories to the fullest extent possible.

For example, in this SIN an offering commercially marketed by a Contractor as “Storage as a Service” would be properly characterized as Infrastructure as a Service (IaaS), storage being a subset of infrastructure. Services commercially marketed as “LAMP as a Service” or “Database as a Service” would be properly characterized under this SIN as Platform as a Service (PaaS), as they deliver two kinds of platform services. Services commercially marketed as “Travel Facilitation as a Service” or “Email as a Service” would be properly characterized as species of Software as a Service (SaaS) for this SIN.

However, Contractors can and should include appropriate descriptions (include commercial marketing terms) of the service in the full descriptions of the service's capabilities.

When choosing between equally plausible service model sub-categories, Contractors should consider several factors:

(1) Visibility to the Ordering Activity. Service model sub-categories in this SIN exist to help Ordering Activities match their requirements with service characteristics. Contractors should select the most intuitive and appropriate service model from the point of view of an Ordering Activity.

(2) Primary Focus of the Cloud Service (i.e. IaaS, etc.). Services may offer a mix of capabilities that span service models in the strict technical sense. For example, a service may offer both IaaS capabilities for processing and storage, along with some PaaS capabilities for application deployment, or SaaS capabilities for specific applications. In a service mix situation the Contractor should select the service model that is their primary focus. Alternatively contractors may choose to submit multiple service offerings for the SIN, each optionally and separately subcategorized.

(3) Ordering Activity Role. Contractors should consider the operational role of the Ordering Activity's primary actual consumer or operator of the service. For example services most often consumed by system managers are likely to fit best as IaaS; services most often consumed by application deployers or developers as PaaS, and services most often consumed by business users as SaaS.

(4) Lowest Level of Configurability. Contractors can consider IaaS, PaaS and SaaS as an ascending hierarchy of complexity, and select the model with the lowest level of available Ordering Activity interaction. As an example, virtual machines are an IaaS service often bundled with a range of operating systems, which are PaaS services. The Ordering Activity usually has access to configure the lower level IaaS service, and the overall service should be considered IaaS. In cases where the Ordering Activity cannot configure the speed, memory, network configuration, or any other aspect of the IaaS component, consider categorizing as a PaaS service.

Cloud management and cloud broker services should be categorized based on their own characteristics and not those of the other cloud services that are their targets. Management and broker services typically fit the SaaS service model, regardless of whether the services they manage are SaaS, PaaS or IaaS. Use Table 3 to determine which service model is appropriate for the cloud management or cloud broker services, or, alternately choose not to select a service model for the service.

The guidance in Table 4 offers examples of how services might be properly mapped to NIST service models and how a Contractor should interpret the service model sub-categories.

**Table 4: Guidance on Mapping to NIST Service Models**

| Service Model | Guidance |
|---|---|
| Infrastructure as a Service (IaaS) | Select an IaaS model for service based equivalents of hardware appliances such as virtual machines, storage devices, routers and other physical devices.<br>● IaaS services are typically consumed by system or device managers who would configure physical hardware in a non-cloud setting<br>● The principal customer interaction with an IaaS service is provisioning then configuration, equivalent to procuring and then configuring a physical device.<br>Examples of IaaS services include virtual machines, object storage, disk block storage, network routers and firewalls, software defined networks.<br>Gray areas include services that emulate or act as dedicated appliances and are directly used by applications, such as search appliances, security appliances, etc. To the extent that these services or their emulated devices provide direct capability to an application they might be better classified as Platform services (PaaS). To the extent that they resemble raw hardware and are consumed by other platform services they are better classified as IaaS. |
| Platform as a Service (PaaS) | Select a PaaS model for service based equivalents of complete or partial software platforms. For the purposes of this classification, consider a platform as a set of software services capable of deploying all or part of an application.<br>● A complete platform can deploy an entire application. Complete platforms can be proprietary or open source<br>● Partial platforms can deploy a component of an application which combined with other components make up the entire deployment<br>● PaaS services are typically consumed by application deployment staff whose responsibility is to take a completed agency application and cause it to run on the designated complete or partial platform service<br>● The principal customer interaction with a PaaS service is deployment, equivalent to deploying an application or portion of an application on a software platform service.<br>● A limited range of configuration options for the platform service may be available.<br>Examples of complete PaaS services include:<br>● A Linux/Apache/MySQL/PHP (LAMP) platform ready to deploy a customer PHP application,<br>● a Windows .Net platform ready to deploy a .Net application,<br>● A custom complete platform ready to develop and deploy an customer application in a proprietary language<br>● A multiple capability platform ready to deploy an arbitrary customer application on a range of underlying software services.<br>The essential characteristic of a complete PaaS is defined by the customer's ability to deploy a complete custom application directly on the platform. |

| | |
|---|---|
| | PaaS includes partial services as well as complete platform services. Illustrative examples of individual platform enablers or components include:<br>● A database service ready to deploy a customer's tables, views and procedures,<br>● A queuing service ready to deploy a customer's message definitions<br>● A security service ready to deploy a customer's constraints and target applications for continuous monitoring<br><br>The essential characteristic of an individual PaaS component is the customer's ability to deploy their unique structures and/or data onto the component for a partial platform function.<br>Note that both the partial and complete PaaS examples all have two things in common:<br>● They are software services, which offer significant core functionality out of the box<br>● They must be configured with customer data and structures to deliver results<br><br>As noted in IaaS, operating systems represent a gray area in that OS is definitely a platform service, but is typically bundled with IaaS infrastructure. If your service provides an OS but allows for interaction with infrastructure, please sub-categorize it as IaaS. If your service "hides" underlying infrastructure, consider it as PaaS. |
| Software as a Service (SaaS) | Select a SaaS model for service based equivalents of software applications.<br>● SaaS services are typically consumed by business or subject-matter staff who would interact directly with the application in a non-cloud setting<br>● The principal customer interaction with a SaaS service is actual operation and consumption of the application services the SaaS service provides.<br><br>Some minor configuration may be available, but the scope of the configuration is limited to the scope and then the permissions of the configuring user. For example an agency manager might be able to configure some aspects of the application for their agency but not all agencies. An agency user might be able to configure some aspects for themselves but not everyone in their agency. Typically only the Contractor would be permitted to configure aspects of the software for all users.<br>Examples of SaaS services include email systems, business systems of all sorts such as travel systems, inventory systems, etc., wiki's, websites or content management systems, management applications that allow a customer to manage other cloud or non-cloud services, and in general any system where customers interact directly for a business purpose.<br>Gray areas include services that customers use to configure other cloud services, such as cloud management software, cloud brokers, etc. In general these sorts of systems should be considered SaaS, per guidance in this document. |

### c. Deployment Model

Deployment models (e.g. private, public, community, or hybrid) are not restricted at the SIN level and any specifications for a deployment model are the responsibility of the Ordering Activity.

Multiple deployment model selection is permitted, but at least one model must be selected. The guidance in Table 4 offers examples of how services might be properly mapped to NIST deployment models and how the Contractor should interpret the deployment model characteristics. Contractors should take care to select the range of NIST deployment models most closely corresponding to each service offered.

Note that the scope of this SIN does not include hardware or software components used to construct a cloud, only cloud capabilities delivered as a service, as noted in the Scope section.

**Table 5: Guidance for Selecting a Deployment Model**

| Deployment Model | Guidance |
|---|---|
| **Private Cloud** | The service is provided exclusively for the benefit of a definable organization and its components; access from outside the organization is prohibited. The actual services may be provided by third parties, and may be physically located as required, but access is strictly defined by membership in the owning organization. |
| **Public Cloud** | The service is provided for general public use and can be accessed by any entity or organization willing to contract for it. |
| **Community Cloud** | The service is provided for the exclusive use of a community with a definable shared boundary such as a mission or interest. As with private cloud, the service may be in any suitable location and administered by a community member or a third party. |
| **Hybrid Cloud** | The service is composed of one or more of the other models. Typically hybrid models include some aspect of transition between the models that make them up, for example a private and public cloud might be designed as a hybrid cloud where events like increased load permit certain specified services in the private cloud to run in a public cloud for extra capacity, e.g. bursting. |

## 6. INFORMATION PERTAINING TO CLOUD RELATED IT PROFESSIONAL SERVICES

### a. SCOPE OF 518210 Cloud Related IT Professional Services

(1) The labor categories, prices, terms and conditions stated under Special Item Numbers 518210 Cloud Services and Related IT Professional Services apply exclusively to this SIN within the scope of this Information Technology Schedule. It is anticipated that the relevant IT Professional Services for this SIN 518210 are related to the following: assessing cloud solutions, preparing for cloud solutions, refactoring legacy solutions for cloud migration, migrating legacy or other systems to cloud solutions, DevOps, developing new cloud based applications and providing management/governance for cloud solutions. Contractors may propose other types of relevant professional services as long as they are specifically designed to work within and/or support the types of cloud product services described in SIN 518210.

(2) Cloud Related IT Professional Services provided under this SIN shall comply with all certifications and industry standards as applicable pertaining to the type of services as specified by ordering agency.

(3) The Contractor shall provide Cloud Related IT Professional Services at the Contractor’s facility and/or at the ordering activity location, as agreed to by the Contractor and the ordering activity.

### b. ORDER

(1) 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 order shall specify the availability of funds and the period for which funds are available.

(2) 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.

### c. PERFORMANCE OF SERVICES

(1) The Contractor shall commence performance of Cloud Related IT Professional Services on the date agreed to by the Contractor and the ordering activity.

(2) The Contractor agrees to render Cloud Related IT Professional Services during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.

(3) The ordering activity should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Cloud Related IT Professional Services shall be completed in a good and workmanlike manner.

(4) Any Contractor travel required in the performance of Cloud Related IT Professional 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.

### d. INSPECTION OF SERVICES

Inspection of services is in accordance with 552.212-4 CONTRACT TERMS AND CONDITIONS– COMMERCIAL ITEMS (JAN 2017) (DEVIATION – FEB 2007) (DEVIATION - FEB 2018) for Firm-Fixed Price orders; or GSAR 552.212-4 CONTRACT TERMS AND CONDITIONS-COMMERCIAL ITEMS (JAN 2017) (DEVIATION - FEB 2018) (ALTERNATE I - JAN 2017) (DEVIATION - FEB 2007) for Time-and-Materials and Labor-Hour Contracts orders placed under this contract.

### e. 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.

### f. 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 Cloud Computing IT Professional Services.

### g. INDEPENDENT CONTRACTOR

All Cloud Computing 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.

### h. ORGANIZATIONAL CONFLICTS OF INTEREST

(1) 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.

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.

**i. INVOICES**

The Contractor, upon completion of the work ordered, shall submit invoices for Cloud Computing 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 IT professional services performed during the preceding month.

**j. PAYMENTS**

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. Payments shall be made in accordance with:

For orders that are NOT time-and-materials/labor hours (fixed price applicable).
● GSAR 552.212-4 CONTRACT TERMS AND CONDITIONS–COMMERCIAL ITEMS (JAN 2017) (DEVIATION – FEB 2007) (DEVIATION - FEB 2018)

For orders that are time-and-materials/labor hours.
● GSAR 552.212-4 CONTRACT TERMS AND CONDITIONS-COMMERCIAL ITEMS (JAN 2017) (DEVIATION - FEB 2018) (ALTERNATE I - JAN 2017) (DEVIATION - FEB 2007)
● FAR 52.216-31 (Feb 2007) Time-and Materials/Labor-Hour Proposal Requirements—Commercial Item Acquisition. As prescribed in 16.601(f)(3), insert the following provision:

(1) The Government contemplates award of a Time-and-Materials or Labor-Hour type of contract resulting from this solicitation.

(2) 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-

i The offeror;

ii Subcontractors; and/or

iii Divisions, subsidiaries, or affiliates of the offeror under a common control.]

**k. RESUMES**

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

**l. 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.

**m. DESCRIPTION OF CLOUD COMPUTING LABOR HOURS AND PRICING**

## CLOUD-RELATED IT PROFESSIONAL SERVICES RATES

## SIN 518210C, SIN 518210C STLOC

| SIN | Labor Category | 11/1/2022-2/19/2023 | 2/20/2023-2/19/2024 |
|---|---|---|---|
| 518210C | Cloud Technical Lead | $181.80 | $189.26 |
| 518210C | Cloud Project Manager | $155.06 | $161.42 |
| 518210C | Cloud Developer I | $96.25 | $100.20 |
| 518210C | Cloud Developer II | $129.40 | $134.71 |
| 518210C | Cloud Developer III | $141.16 | $146.94 |
| 518210C | Senior Cloud Developer | $163.63 | $170.34 |
| 518210C | Cloud Architect | $171.11 | $178.13 |
| 518210C | Senior Cloud Architect | $181.80 | $189.26 |
| 518210C | Principal Cloud Architect | $196.77 | $204.84 |
| 518210C | Cloud Engineer I | $96.25 | $100.20 |
| 518210C | Cloud Engineer II | $133.67 | $139.15 |
| 518210C | Cloud Engineer III | $165.76 | $172.56 |
| 518210C | Cloud Network Engineer II | $126.19 | $131.36 |
| 518210C | Cloud Systems Analyst II | $128.33 | $133.59 |
| 518210C | Cloud Services Subject Matter Expert II | $196.77 | $204.84 |
| 518210C | Cloud Services Subject Matter Expert III | $236.34 | $246.04 |

# SIN 518210C & 518210CSTLOC
# Cloud-Related IT Professional Services

## Job Title: Cloud Technical Lead

**Functional Duties/Responsibilities:** Leads the development, architecture and engineering teams to build cloud systems and cloud-related applications in compliance with the SELC lifecycle. Anticipates and resolves issues and risks; ensures the programs are delivered with high quality; contributes to the development and continuous review of appropriate practices, standards and guidelines. Manages, plans, schedules, communicates, facilitates, monitors, and controls architecture, engineering and development related tasks. Determines, monitors, and reviews program economics to include, staffing requirements, resources and risk. Plans, schedules, monitors, and reports on activities related to the program. Establishes appropriate metrics for measuring key program criteria. Manages the integration of products into the overall program schema. Oversees the application of products.

**Education/Experience Required:** A Bachelor's degree in computer science, information systems, business, engineering or related scientific or technical discipline. This position requires a minimum of four (4) years cloud-related experience, and a minimum of four (4) years as a project manager. Experience includes increasing responsibilities in program and project management and cloud systems design. Scrum experience or certification is desired.

## Job Title: Cloud Project Manager

**Functional Duties/Responsibilities:** On a cloud-related project, manages, plans, schedules, communicates, facilitates, monitors, and controls project related tasks to ensure timely implementation of releases through deployment, and, in accordance with Project Management standards and procedures. Determines, monitors, and reviews all project economics to include costs, operational budgets, staffing requirements, sub-contractors, resources and risk. Plans, schedules, monitors, and reports on activities related to the project. Leads the project team(s) in determining client requirements and translating requirements into operational plans. Controls project requirements, scope, and change management issues. Coaches members of cross-functional teams to accomplish project goals, to meet established schedules, and resolve technical/operational issues. Establishes appropriate metrics for measuring key program criteria. These responsibilities include managing cross-functional teams, and delivering approved projects on time, within budget, and with quality results.

**Education/Experience Required:** A Bachelor's degree in computer science, information systems, business, engineering or related scientific or technical discipline. This position requires a minimum of two (2) years project management experience, one (1) of which must be as a project manager in a cloud environment. Scrum experience or certification is desired.

## Job Title: Cloud Developer I

**Functional Duties/Responsibilities**: Under general direction, designs, modifies, develops and implements cloud-related software programming applications. Understands and applies Agile DevSecOps practices. Uses structured programming, and other development applications. Develops design documentation using industry standard modeling techniques and methodologies. Tests, debugs, and refines the code and software.

**Education/Experience Required:** Associate's degree and two (2) years of technical experience. Experience with cloud-based systems preferred.

### Job Title: Cloud Developer II

Functional Duties/Responsibilities: Under minimal direction, designs, modifies, develops and implements cloud-related software programming applications. Understands and applies Agile DevSecOps practices. Has knowledge of cloud PaaS services and how to integrate them into modern application development. Uses structured programming, other development applications, automation, microservices, serverless development, and container service development. Develops design documentation using industry standard modeling techniques and methodologies. Tests, debugs, and refines the code and software.

**Education/Experience Required:** A Bachelor's degree in Computer Science, Information Systems, Engineering, or a related discipline and three (3) years of DevSecOps experience including at least two (2) years of experience in cloud-based applications.

### Job Title: Cloud Developer III

**Functional Duties/Responsibilities:** Under broad direction, designs, modifies, develops and implements cloud-related software solutions to meet client requirements. Demonstrated broad experience in Agile DevSecOps to include software system development, design, and testing, programming, software maintenance, configuration management, and documentation. Plans, designs, develops, tests, maintains, and documents software applications and systems. Has a working knowledge of System Development Life Cycle (SDLC) Management, system analysis, structured programming, version control, quality assurance, methodologies, software testing, documentation, and end user support.

**Education/Experience Required:** A Bachelor's degree in Computer Science, Information Systems, Engineering, or a related discipline and five (5) years of DevSecOps experience including at least three (3) years of experience in cloud-based applications.

### Job Title: Senior Cloud Developer

**Functional Duties/Responsibilities:** Under broad direction, designs, modifies, develops and implements cloud-related software solutions to meet client requirements. Demonstrated broad experience in Agile software development to include software system development, design, and testing, programming, software maintenance, configuration management, and documentation. Plans, designs, develops, tests, maintains, and documents software applications and systems. Has a working knowledge of System Development Life Cycle (SDLC) Management, system analysis, structured programming, version control, quality assurance, methodologies, software testing, documentation, and end user support. Leads and directs a team of developers as part of a larger software development effort.

**Education/Experience Required:** A Bachelor's degree in Computer Science, Information Systems, Engineering, or a related discipline and five (5) years of DevSecOps experience including at least three (3) years of experience in cloud-based applications.

### Job Title: Cloud Architect

Functional Duties/Responsibilities: Under minimal direction, collaborates with end-users to define, analyze and review business requirements for cloud-related projects. Collaborates with the technical team to define technical specifications and system design; develop technical and data architecture for securing and delivering information systems in a public cloud. Partners with all aspects of the business/ business units (BUs) to help align business goals to technical architecture for the program. Partners with IT management to establish and institutionalize processes and procedures for demand management and development resource allocation; leads the development and deployment activities; facilitates design reviews and code walkthroughs; organizes and participates in testing activities to ensure delivery of quality systems; prepares and manages project plans and milestones; estimates level of effort and resource utilization; anticipates and resolves issues and risks; ensures the projects are delivered with high quality; contributes to the development and continuous review of appropriate practices, standards and guidelines.

**Education/Experience Required:** BS degree in Computer Science or related field and four (4) years of technical experience including at least two (2) years of experience with architecture of cloud-based systems.

### Job Title: Senior Cloud Architect

**Functional Duties/Responsibilities:** Under broad direction, collaborates with end-users to define, analyze and review business requirements for cloud-related projects. Collaborates with the technical team to define technical specifications and system design. Partners with all aspects of the business/ business units (BUs) to help align business goals to technical architecture for the program. Partners with IT management to establish and institutionalize processes and procedures for demand management and development resource allocation; leads the development and deployment activities; facilitates design reviews and code walkthroughs; organizes and participates in testing activities to ensure delivery of quality systems; prepares and manages project plans and milestones; estimates level of effort and resource utilization; anticipates and resolves issues and risks; ensures the projects are delivered with high quality; contributes to the development and continuous review of appropriate practices, standards and guidelines. Leads and directs a team of architects as part of a larger effort.

**Education/Experience Required:** BS degree in Computer Science or related field and five (5) years of technical experience including at least three (3) years of experience with architecture of cloud-based systems.

### Job Title: Principle Cloud Architect

**Functional Duties/Responsibilities:** Provides technical/management leadership on major tasks or technology assignments involving cloud-related IT operations. Partners with all aspects of the business/ business units (BUs) to help align business goals to technical architecture for the program. Partners with IT management to establish and institutionalize processes and procedures for demand management and development resource allocation; leads the development and deployment activities; facilitates design reviews and code walkthroughs; organizes and participates in testing activities to ensure delivery of quality systems; prepares and manages project plans and milestones; estimates level of effort and resource utilization; anticipates and resolves issues and risks; ensures the projects are delivered with high quality; contributes to the development and continuous review of appropriate practices, standards and guidelines. Leads and directs a team of architects as part of a larger effort. Provide subject matter expertise on the various cloud systems and applications.

**Education/Experience Required:** Bachelor's degree in Computer Science or related field and eight (8) years of technical experience including at least five (5) years of experience with architecture of cloud-based systems.

### Job Title: Cloud Engineer I

**Functional Duties/Responsibilities:** Under general direction, responsible for the technical implementation of the assigned cloud solution, according to the relevant customer's specification and the current requirements. Works with product management to define requirements; works with engineering to define the design for a cloud solution; ensures designs achieve high availability, maintainability and reliability of the product; helps define the future system cloud architecture leading to increased capacity and availability.

**Education/Experience Required:** Associate's degree and two (2) years of technical experience. Experience with cloud-based systems preferred.

### Job Title: Cloud Engineer II

**Functional Duties/Responsibilities:** Under minimal direction, integrates a broad range of cloud solutions in support of client requirements for cloud-related IT projects. Formulates and defines system scope and objectives, develops and modifies processes to solve issues for cloud-based systems to achieve desired results. Engineers systems for highly available, fault tolerate configurations aligning toward scalable and durable platforms. Develops and applies engineering and design methods in the investigation and solution of cloud system requirements, hardware/software interfaces and applications and solutions. Responsible for design, development, engineering, and integration of cloud-based systems.

**Education/Experience Required:** Bachelor's degree in Computer Science, MIS or related field and three (3) years technical experience with emphasis on cloud-based systems.

### Job Title: Cloud Engineer III

**Functional Duties/Responsibilities:** Under broad direction, integrates a broad range of cloud solutions in support of client requirements for cloud-related IT projects. Formulates and defines system scope and objectives, develops and modifies processes to solve complex problems for cloud-based systems to achieve desired results using innovative technologies. Engineers systems for highly available, fault tolerate configurations aligning toward scalable and durable platforms. Develops and applies advanced engineering and design methods, theories, and research techniques in the investigation and solution of complex and advanced cloud system requirements, hardware/software interfaces and applications and solutions. Responsible for design, development, engineering, integration, and architecture of cloud-based systems. Manages the technical development work on complex cloud-based projects with the application of new and unique technologies. Provides technical leadership.

**Education/Experience Required:** Bachelor's degree in Computer Science, MIS or related field and eight (8) years technical experience including at least five (5) years of engineering experience with cloud-based systems.

### Job Title: Cloud Network Engineer II

**Functional Duties/Responsibilities:** Under minimal direction, implements and administers cloud solutions which meet customer business requirements and service level agreements; monitors, and enforces cloud network security systems; monitors and manages cloud network availability and performance to substantiate defined service level agreements; evaluates cloud network hardware, software, and cloud-native services solutions in accordance to industry standards; manages and monitors firewall products; participates in regular cloud network maintenance activities. Installs, maintains, and monitors the operation of the organization's cloud network and acts as liaison between developers, operators, vendors, customers, and other personnel regarding the issues surrounding cloud network hardware, software, and cloud-native services.

**Education/Experience Required:** Bachelor's degree in Computer Science, MIS or related field and three (3) years of experience managing cloud networks.

### Job Title: Cloud Systems Analyst II

**Functional Duties/Responsibilities:** Under minimal direction, responsible for cloud systems process analysis and design. Requires understanding of organization's business systems and industry requirements. Provides guidance and insight into specific cloud technologies and their application and independently performs a variety of system design and integration tasks where a specific subject matter expertise is necessary. Plans and performs research, design assessment, development, integration and other assignments in a specific technical area. Creates process change by integrating new processes with existing ones and communicating these changes to impacted teams. Recommends and facilitates quality improvement efforts.

**Education/Experience Required:** Bachelor's degree in Business Information Systems, Computer Science, or a related field and three (3) years of experience including at least two (2) years of experience **i**n cloud-related requirements analysis and documentation.

### Job Title: Cloud Services Subject Matter Expert II

**Functional Duties/Responsibilities:** Leads technical team in specific technical niches to design federal enterprise-level cloud-based systems and applications in compliance with government standards and in sync with the full system lifecycle. Collaborates with end-users and other system administrators to define, analyze and review business requirements; Collaborates with the technical team to define technical specifications and cloud system design; partners with IT management to establish and institutionalize processes and procedures for demand management and development resource allocation; leads the development and deployment activities; facilitates design reviews and code walkthroughs; organizes and participates in testing activities to ensure delivery of quality systems; prepares and manages cloud-related project plans and milestones; estimates level of effort and resource utilization; anticipates and resolves issues and risks; acts as team developer lead on projects with multiple developers; ensures the projects are delivered with high quality; contributes to the development and continuous review of appropriate practices, standards and guidelines.

**Education/Experience Required:** Bachelor's Degree and ten (10) years of technical experience with at least five (5) years of experience with cloud-based technical solutions. Familiar with government cloud standards and has specific domain expertise.

### Job Title: Cloud Services Subject Matter Expert III

**Functional Duties/Responsibilities:** Leads technical team in specific technical niches to design federal enterprise-level cloud-based systems and applications in compliance with government standards and in sync with the full system lifecycle. Collaborates with end-users and other system administrators to define, analyze and review business requirements; Collaborates with the technical team to define technical specifications and cloud system design; partners with IT management to establish and institutionalize processes and procedures for demand management and development resource allocation; leads the development and deployment activities; facilitates design reviews and code walkthroughs; organizes and participates in testing activities to ensure delivery of quality systems; prepares and manages cloud-related project plans and milestones; estimates level of effort and resource utilization; anticipates and resolves issues and risks; acts as team developer lead on projects with multiple developers; ensures the projects are delivered with high quality; contributes to the development and continuous review of appropriate practices, standards and guidelines.

**Education/Experience Required:** Bachelor's Degree and fifteen (15) years of technical experience with at least 5 years of experience with cloud-based technical solutions. Expert in Government cloud standards and has extensive domain expertise.

**Education/Experience Substitution Table**

| DEGREE | DEGREE AND EXPERIENCE SUBSTITUTION | RELATED EXPERIENCE SUBSTITUTION |
|---|---|---|
| **Associate's** | **2 Years** | **2 Years** |
| **Bachelor's** | **Associate's + 2 Years** | **4 Years** |
| **Master's** | **Bachelor's + 2 Years** | **6 Years** |
| **Doctorate** | **Master's + 2 Years** | **8 Years** |

## TERMS AND CONDITIONS APPLICABLE TO INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 54151S); HIGHLY AVAILABLE CYBERSECURITY SERVICES (SPECIAL ITEM NUMBER 54151HACS); IDENTITY, CREDENTIALING AND ACCESS MANAGEMENT (ICAM) PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 541519ICAM)

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

### 1. SCOPE

a. The prices, terms and conditions stated under Special Item Numbers 54151S, 54151HACS, and 541519ICAM Professional Services apply exclusively to IT, HACS, and ICAM Professional Services within the scope of this GSA 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. 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.

### 3. SERVICES PERFORMED

a. 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.

b. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity.

c. The Contractor agrees to render services only during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.

### 4. TRAVEL

Any Contractor travel required in the performance of IT Services must comply with the Pub. L. 99-234 and FAR Part 31.205-46, as applicable,, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel.

(2) Subcontractors; and/or

(3) Divisions, subsidiaries, or affiliates of the offeror under a common control.

### 5. WARRANTY

a. Unless otherwise specified in the contract, the Contractor's standard commercial warrantyapplies.

b. The Contractor's commercial guarantee/warranty shall be included in the Commercial SupplierAgreement to include Enterprise User License Agreements or Terms of Service (TOS) Agreements, if applicable.

c. Except as otherwise provided by an express or implied warranty, the Contractor will not be liable to the ordering activity for consequential damages resulting from any defect or deficiencies in accepted items.

### 6. INVOICES

All services shall be billed in arrears in accordance with 31 U.S.C. 3324.

### 7. RESUMES

Resumes shall be provided to the GSA contracting officer or the user ordering activity upon request.

**Regulation Number Regulation Title/Comments**
52.222-46 EVALUATION OF COMPENSATION FOR PROFESSIONAL EMPLOYEES (FEB 1993)
52.222-48 EXEMPTION FROM APPLICATION OF THE SERVICE CONTRACT LABOR STANDARDS TO CONTRACTS FOR MAINTENANCE, CALIBRATION, OR REPAIR OF CERTAIN EQUIPMENT CERTIFICATION (MAY 2014)

52.223-19 COMPLIANCE WITH ENVIRONMENTAL MANAGEMENT SYSTEMS (MAY 2011)
52.223-2 AFFIRMATIVE PROCUREMENT OF BIOBASED PRODUCTS UNDER SERVICE AND CONSTRUCTION CONTRACTS (SEP 2013)
52.229-1 STATE AND LOCAL TAXES (APR 1984)
52.222-62 PAID SICK LEAVE UNDER EXECUTIVE ORDER 13706 (JAN 2022)
52.223-13 ACQUISITION OF EPEAT - REGISTERED IMAGING EQUIPMENT (JUN 2014)
52.223-14 ACQUISITION OF EPEAT® - REGISTERED TELEVISIONS (JUN 2014)
52.223-16 ACQUISITION OF EPEAT® - REGISTERED PERSONAL COMPUTER PRODUCTS (OCT 2015)
552.238-115 SPECIAL ORDERING PROCEDURES FOR THE ACQUISITION OF ORDER-LEVEL MATERIALS (APR 2022)
552.238-107 TRAFFIC RELEASE (SUPPLIES) (MAY 2019)
552.238-73 IDENTIFICATION OF ELECTRONIC OFFICE EQUIPMENT PROVIDING ACCESSIBILITY FOR INDIVIDUALS WITH DISABILITIES (MAR 2022)
552.238-86 DELIVERY SCHEDULE (MAY 2019)
552.238-89 DELIVERIES TO THE U.S. POSTAL SERVICE (MAY 2019)
552.238-90 CHARACTERISTICS OF ELECTRIC CURRENT (MAY 2019)
552.238-91 MARKING AND DOCUMENTATION REQUIREMENTS FOR SHIPPING (MAY 2019)
552.238-92 VENDOR MANAGED INVENTORY (VMI) PROGRAM (MAY 2019)
552.238-93 ORDER ACKNOWLEDGMENT (MAY 2019)
552.238-94 ACCELERATED DELIVERY REQUIREMENTS (MAY 2019)

DESCRIPTION OF IT PROFESSIONAL SERVICES AND PRICING

## IT PROFESSIONAL SERVICES RATES

## SIN 54151S, SIN 54151SSTLOC

| SIN | Labor Category | 11/1/2022 – 2/19/22 | 2/20/23 - 2/19/24 |
|---|---|---|---|
| 54151S | Project Manager | $155.98 | $162.38 |
| 54151S | Senior Developer | $166.89 | $173.73 |
| 54151S | Developer III | $143.99 | $149.89 |
| 54151S | Developer II | $131.99 | $137.40 |
| 54151S | Enterprise Architect | $201.79 | $210.07 |
| 54151S | Senior Solutions Architect | $174.52 | $181.67 |
| 54151S | Solutions Architect | $169.08 | $176.01 |
| 54151S | Systems Engineer II | $131.99 | $137.40 |
| 54151S | Systems Engineer I | $109.08 | $113.55 |
| 54151S | Associate Systems Engineer | $98.18 | $102.21 |
| 54151S | Network Engineer II | $119.99 | $124.91 |
| 54151S | Functional Systems Analyst II | $130.89 | $136.26 |
| 54151S | Functional Systems Analyst I | $91.63 | $95.39 |
| 54151S | Subject Matter Expert III | $241.07 | $250.95 |
| 54151S | Subject Matter Expert II | $200.71 | $208.94 |
| 54151S | Privacy Subject Matter Expert | $233.13 | $242.69 |
| 54151S | Senior Privacy Analyst | $170.67 | $177.66 |
| 54151S | Privacy Analyst | $132.52 | $137.95 |

# IT PROFESSIONAL SERVICES
# SIN 54151S and 54151SSTLOC

### Job Title: Project Manager

**Functional Duties/Responsibilities:** Channels the performance of (a) task/tasks on a related program. Manages the integration of products into the overall program schema. Oversees the application of products. Responsible for managing, planning, scheduling, communicating, facilitating, monitoring, controlling, and reporting project related tasks to ensure timely implementation of releases through deployment, and, in accordance with Project Management standards and procedures. These responsibilities include managing cross-functional teams, and delivering approved projects on time, within budget, and with quality results.

**Education/Experience Required:** A Bachelor's degree in computer science, information systems, business, engineering or related scientific or technical discipline. This position requires a minimum of two (2) years general related experience, one (1) of which must be as a project manager. Experience includes increasing responsibilities in program and project management and information systems design.

### Job Title: Senior Developer

**Functional Duties/Responsibilities:** Designs, modifies, develops and implements software solutions to meet client requirements. Demonstrated broad experience in software development to include software system development, design, and testing, programming, software maintenance, configuration management, and documentation. Plans, designs, develops, tests, maintains, and documents software applications and systems. Follows client's SDLC methodology and software engineering standards. Working knowledge of System Development Life Cycle (SDLC) Management, system analysis, structured programming, version control, quality assurance, methodologies, software testing, documentation, and end user support. Supervises and provides direction to software engineers as required.

**Education/Experience Required:** A Bachelor's degree in Computer Science, Information Systems, Engineering, or a related discipline and five (5) years of technical experience with ability to lead team of developers on IT projects.

### Job Title: Developer III

**Functional Duties/Responsibilities:** Designs, modifies, develops and implements software solutions to meet client requirements. Demonstrated broad experience in software development to include software system development, design, and testing, programming, software maintenance, configuration management, and documentation. Plans, designs, develops, tests, maintains, and documents software applications and systems. Follows client's SDLC methodology and software engineering standards. Working knowledge of System Development Life Cycle (SDLC) Management, system analysis, structured programming, version control, quality assurance, methodologies, software testing, documentation, and end user support.

**Education/Experience Required:** A Bachelor's degree in Computer Science, Information Systems, Engineering, or a related discipline and five (5) years of IT technical experience.

### Job Title: Developer II

**Functional Duties/Responsibilities:** Designs, modifies, develops and implements software programming applications. Uses structured programming, and other development applications. Develops Block diagrams and logic flow charts. Tests, debugs, and refines the code and software.

**Education/Experience Required:** A Bachelor's degree in Computer Science, Information Systems, Engineering, or a related discipline and three (3) years of IT technical experience.

### Job Title: Enterprise Architect

**Functional Duties/Responsibilities:** Leads the development team to build enterprise systems and applications in compliance with the full system lifecycle. Collaborates with end-users to define, analyze and review business requirements; Collaborates with the technical team to define technical specifications and system design; partners with IT management to establish and institutionalize processes and procedures for demand management and development resource allocation; leads the development and deployment activities; facilitates design reviews and code walkthroughs; organizes and participates in testing activities to ensure delivery of quality systems; prepares and manages project plans and milestones; estimates level of effort and resource utilization; anticipates and resolves issues and risks; acts as team developer lead on projects with multiple developers; ensures the projects are delivered with high quality; contributes to the development and continuous review of appropriate practices, standards and guidelines.

**Education/Experience Required:** BS degree in Computer Science or related field and eight (8) years of technical experience with emphasis on enterprise IT systems and applications.

### Job Title: Senior Solutions Architect

**Functional Duties/Responsibilities:** Leads the development team to build enterprise systems and applications in compliance with the full system lifecycle. Collaborates with end-users to define, analyze and review business requirements; Collaborates with the technical team to define technical specifications and system design; partners with IT management to establish and institutionalize processes and procedures for demand management and development resource allocation; leads the development and deployment activities; facilitates design reviews and code walkthroughs; organizes and participates in testing activities to ensure delivery of quality systems; prepares and manages project plans and milestones; estimates level of effort and resource utilization; anticipates and resolves issues and risks; acts as team developer lead on projects with multiple developers; ensures the projects are delivered with high quality; contributes to the development and continuous review of appropriate practices, standards and guidelines.

**Education/Experience Required:** BS degree in Computer Science or related field and four (4) years of technical experience with emphasis on the architecture of IT systems and applications.

### Job Title: Solutions Architect

**Functional Duties/Responsibilities:** Collaborates with end-users to define, analyze and review business requirements; Collaborates with the technical team to define technical specifications and system design; partners with IT management to establish and institutionalize processes and procedures for demand management and development resource allocation; leads the development and deployment activities; facilitates design reviews and code walkthroughs; organizes and participates in testing activities to ensure delivery of quality systems; prepares and manages project plans and milestones; estimates level of effort and resource utilization; anticipates and resolves issues and risks; ensures the projects are delivered with high quality; contributes to the development and continuous review of appropriate practices, standards and guidelines.

**Education/Experience Required:** BS degree in Computer Science or related field and four (4) years of technical IT experience.

### Job Title: Systems Engineer II

**Functional Duties/Responsibilities:** Responsible for the technical implementation of the assigned system, across company's projects, according to the relevant customer's specification and the current requirements. Works with senior management; works with engineering to define the high-level design for a complex real time system; ensures designs achieve high availability, maintainability and reliability of the product; helps define the future system architecture leading to increased capacity and availability.

**Education/Experience Required:** A BS degree in Computer Science or a related field and three (3) years of IT technical experience.

### Job Title: Systems Engineer I

**Functional Duties/Responsibilities:** Responsible for the technical implementation of the assigned system, across company's projects, according to the relevant customer's specification and the current requirements. Works with Product management to define requirements; works with engineering to define the high-level design for a real time system; ensures designs achieve high availability, maintainability and reliability of the product; helps define the future system architecture leading to increased capacity and availability.

**Education/Experience Required:** A BS degree in Computer Science or a related field and one (1) year of IT technical experience.

### Job Title: Associate Systems Engineer

**Functional Duties/Responsibilities:** Responsible for the technical implementation of the assigned system, across company's projects, according to the relevant customer's specification and the current requirements. Works with Product management to define requirements; works with engineering to define the high-level design for a real time system; ensures designs achieve high availability, maintainability and reliability of the product; helps define the future system architecture leading to increased capacity and availability.

**Education/Experience Required:** Associate's degree and two (2) years of IT technical experience.

### Job Title: Network Engineer II

**Functional Duties/Responsibilities:** Implements and administers network solutions which meet customer business requirements and service level agreements; monitors, and enforces network security systems; monitors and manages network availability and performance to substantiate defined service level agreements; evaluates network hardware and software solutions in accordance to industry standards; manages and monitors network firewall products; participates in regular network maintenance activities. Installs, maintains, and monitors the operation of the organization's enterprise network and acts as liaison between developers, operators, vendors, customers, and other personnel regarding the issues surrounding network hardware and software.

**Education/Experience Required:** BS degree in Computer Science, MIS or related field and three (3) years experience managing networks.

### Job Title: Functional Systems Analyst II

**Functional Duties/Responsibilities:** Under broad direction, responsible for systems process analysis and design. Requires understanding of organization's business systems and industry requirements. Provides guidance and insight into specific technologies and their application and independently performs a variety of system design and integration tasks where a specific subject matter expertise is necessary. Plans and performs research, design assessment, development, integration and other assignments in a specific technical area. Creates process change by integrating new processes with existing ones and communicating these changes to impacted teams. Recommends and facilitates quality improvement efforts.

**Education/Experience Required:** BS degree in Business Information Systems, Computer Science, or a related field and five (5) years of experience in requirements analysis and documentation.

### Job Title: Functional Systems Analyst I

**Functional Duties/Responsibilities** Under direct supervision, responsible for systems process analysis and design. Plans and performs research, design assessment, development, integration and other assignments in a specific technical area. Analyzes problems for resolution, gathers information from client users, defines work problems, and, if feasible, designs a system of computer programs and procedures to resolve the problems. Creates process change by integrating new processes with existing ones and communicating these changes to impacted teams. Recommends and facilitates quality improvement efforts.

**Education/Experience Required:** Associate's degree in Business Information Systems, Computer Science, or a related field and two (2) years of technical experience.

### Job Title: Subject Matter Expert III

**Functional Duties/Responsibilities:** Leads development team in specific technical niches to design federal enterprise-level systems and applications in compliance with government standards and in sync with the full system lifecycle. Collaborates with end-users and other system administrators to define, analyze and review business requirements; Collaborates with the technical team to define technical specifications and system design; partners with IT management to establish and institutionalize processes and procedures for demand management and development resource allocation; leads the development and deployment activities; facilitates design reviews and code walkthroughs; organizes and participates in testing activities to ensure delivery of quality systems; prepares and manages project plans and milestones; estimates level of effort and resource utilization; anticipates and resolves issues and risks; acts as team developer lead on projects with multiple developers; ensures the projects are delivered with high quality; contributes to the development and continuous review of appropriate practices, standards and guidelines.

**Education/Experience Required:** Bachelor's Degree and fifteen (15) years of technical experience with emphasis on subject specific technical solutions.

### Job Title: Subject Matter Expert II

**Functional Duties/Responsibilities:** Leads development team in specific technical niches to design federal enterprise-level systems and applications in compliance with government standards and in sync with the full system lifecycle. Collaborates with end-users and other system administrators to define, analyze and review business requirements; Collaborates with the technical team to define technical specifications and system design; partners with IT management to establish and institutionalize processes and procedures for demand management and development resource allocation; leads the development and deployment activities; facilitates design reviews and code walkthroughs; organizes and participates in testing activities to ensure delivery of quality systems; prepares and manages project plans and milestones; estimates level of effort and resource utilization; anticipates and resolves issues and risks; acts as team developer lead on projects with multiple developers; ensures the projects are delivered with high quality; contributes to the development and continuous review of appropriate practices, standards and guidelines.

**Education/Experience Required:** Bachelor's Degree and ten (10) years of technical experience with emphasis on subject specific technical solutions.

### Job Title: Privacy SME

**Functional Duties/Responsibilities:** Provides expert level understanding related to privacy based on experience in one or more of the critical infrastructure sectors. Includes knowledge of and experience with the legal and regulatory privacy-related cybersecurity frameworks associated with respective critical infrastructure sectors, especially as related to executive-level risk management, common cybersecurity practices, and cybersecurity tools and metrics. Applies subject matter expertise to high-level analysis, and guidance development for cybersecurity challenges. Applies high-level facilitation skills within large groups in order to derive stakeholder cybersecurity imperatives and support the prioritization of sometimes competing privacy-related cybersecurity imperatives.

**Education/Experience Required:** A Bachelor's degree in computer science, information systems, business, engineering or related scientific or technical discipline.  Bachelor's Degree and ten (10) years of technical experience with at least 8 years of experience with privacy technical solutions. Expert in Government privacy standards and has extensive domain expertise.

### Job Title: Senior Privacy Analyst

**Functional Duties/Responsibilities:** Under broad direction, assists with applying subject matter expertise to high-level analysis, and guidance development for privacy-related cybersecurity challenges. Familiar with federal guidelines for the Privacy requirements and expertise in complying with and applying guidance (e.g, FISMA,NIST, OMB). Conducts interviews with appropriate stakeholders and prepares privacy analyses, privacy risk assessments, and privacy impact assessments, as applicable to analyze new or proposed changes to existing technology, sharing agreements, and programs to identify privacy risks and provide possible mitigation strategies. Performs assessments and analyses of projects and studies that require analysis of interrelated issues such as legal compliance, policy compliance, and regulatory compliance. Gathers relevant information concerning systems collecting personally identifiable information to determine applicable regulatory requirements and drafts compliance documentation in accordance with requirements.  Participates in product development meetings to identify privacy equities.

**Education/Experience Required:** A Bachelor's degree in computer science, information systems, business, engineering or related scientific or technical discipline.  Bachelor's Degree and seven (7) years of technical experience with at least 5 years of experience with privacy technical solutions. Expert in Government privacy standards.

### Job Title: Privacy Analyst

**Functional Duties/Responsibilities:** Under general direction, assists with applying subject matter expertise to privacy-related cybersecurity challenges. Familiar with federal guidelines for the Privacy requirements and compliance and applying guidance (e.g, FISMA,NIST, OMB). Conducts interviews with appropriate stakeholders and prepares privacy analyses, privacy risk assessments, and privacy impact assessments, as applicable to analyze new or proposed changes to existing technology, sharing agreements, and programs to identify privacy risks and provide possible mitigation strategies. Performs assessments and analyses of projects and studies that require analysis of interrelated issues such as legal compliance, policy compliance, and regulatory compliance. Gathers relevant information concerning systems collecting personally identifiable information to determine applicable regulatory requirements and drafts compliance documentation in accordance with requirements. Participates in product development meetings to identify privacy equities.

**Education/Experience Required:** A Bachelor's degree in computer science, information systems, business, engineering or related scientific or technical discipline. Bachelor's Degree and four (4) years of technical experience with at least 3 years of experience with privacy technical solutions.

## HIGHLY AVAILABLE CYBERSECURITY SERVICES RATES

## SIN 54151HACS, SIN 54151HACSSTLOC

| SIN | Labor Category | 10/13/22 - 2/19/23 | 2/20/23 - 2/19/24 |
|---|---|---|---|
| 54151HACS | Associate Cybersecurity Analyst | $82.64 | $86.03 |
| 54151HACS | Cybersecurity Analyst | $113.69 | $118.35 |
| 54151HACS | Senior Cybersecurity Analyst | $123.05 | $128.10 |
| 54151HACS | Cybersecurity Engineer II | $129.64 | $134.96 |
| 54151HACS | Cybersecurity Engineer III | $187.14 | $194.82 |
| 54151HACS | Cybersecurity Subject Matter Expert I | $158.16 | $164.64 |
| 54151HACS | Cybersecurity Subject Matter Expert II | $196.35 | $204.40 |
| 54151HACS | Cybersecurity Subject Matter Expert III | $215.73 | $224.57 |
| 54151HACS | Cybersecurity Subject Matter Expert IV | $330.78 | $344.34 |
| 54151HACS | Cybersecurity Project Manager | $144.31 | $150.23 |
| 54151HACS | Cybersecurity Program Manager | $160.68 | $167.26 |

## HIGHLY AVAILABLE CYBERSECURITY SERVICES
## SIN 54151HACS and 54151HACSSTLOC

### Job Title: Associate Cybersecurity Analyst

**Functional Duties/Responsibilities:** Under supervision, collaborates with end users to provide assessment and security engineering solutions. Supports the development and deployment activities;

supports and participates in testing activities to ensure delivery of quality systems;  contributes to the development and continuous review and testing of appropriate cybersecurity practices, standards and guidelines.

**Education/Experience Required:** Associate's degree and two (2) years of IT technical experience.

### Job Title: Cybersecurity Analyst

**Functional Duties/Responsibilities:** Under supervision, collaborates with end users to provide assessment and security engineering solutions.  Supports the development and deployment activities; supports and participates in testing activities to ensure delivery of quality systems;  contributes to the development and continuous review and testing of appropriate cybersecurity practices, standards and guidelines.

**Education/Experience Required:** BS degree in Computer Science or a related field and  one (1) year of IT technical experience.

### Job Title: Senior Cybersecurity Analyst

**Functional Duties/Responsibilities:** Under general direction, collaborates with end users to provide assessment and security engineering solutions.  Supports the development and deployment activities; supports and participates in testing activities to ensure delivery of quality systems;  contributes to the development and continuous review and testing of appropriate cybersecurity practices, standards and guidelines.

**Education/Experience Required:** BS degree in Computer Science or a related field and three (3) years of IT technical experience.

### Job Title: Cybersecurity Engineer II

**Functional Duties/Responsibilities:** Under general direction, collaborates with end-users to define, analyze and review requirements for cybersecurity  projects. Collaborates with the technical team to define technical specifications, test parameters, and system design. Partners with the business/ business units  to help align business goals to security architecture for the program. Partners with IT management to establish and institutionalize processes and procedures for cybersecurity; supports the development and deployment activities; facilitates design reviews and code walkthroughs; supports and participates in testing activities to ensure delivery of quality systems; prepares and manages project plans and milestones; estimates level of effort and resource utilization; anticipates and resolves issues and risks; ensures the projects are delivered with high quality; contributes to the development and continuous review of appropriate cybersecurity practices, standards and guidelines.  Conducts RMF services, security assessments and testing.

**Education/Experience Required:** BS degree in Computer Science or a related field and five (5) years of IT technical experience with an emphasis in cybersecurity.

### Job Title: Cybersecurity Engineer III

**Functional Duties/Responsibilities:** Under minimal  direction, collaborates with end-users to define, analyze and review requirements for cybersecurity  projects. Collaborates with the technical team to define technical specifications, test parameters, and system design. Partners with the business/ business units  to help align business goals to security architecture for the program. Partners with IT management to establish and institutionalize processes and procedures for cybersecurity; supports the development and deployment activities; facilitates design reviews and code walkthroughs; supports and participates in testing activities to ensure delivery of quality systems; prepares and manages project plans and milestones; estimates level of effort and resource utilization; anticipates and resolves issues and risks; ensures the projects are delivered with high quality; contributes to the development and continuous review of appropriate cybersecurity practices, standards and guidelines.  Conducts RMF services, security assessments and testing.

**Education/Experience Required:** BS degree in Computer Science or a related field and eight (8) years of IT technical experience with an emphasis in cybersecurity.

### Job Title: Cybersecurity Subject Matter Expert I

**Functional Duties/Responsibilities:** Under minimal direction, provides advanced level understanding related to cybersecurity. Includes familiarity with the legal and regulatory privacy-related cybersecurity frameworks associated with respective critical infrastructure sectors, especially as related to common cybersecurity practices, assessment and testing methodologies,and cybersecurity tools and metrics. Applies subject matter expertise to high-level analysis, and guidance development for cybersecurity challenges.

**Education/Experience Required:** BS degree in Computer Science or a related field and five (5) years of IT technical experience including at least three (3) years of experience in cybersecurity.

### Job Title: Cybersecurity Subject Matter Expert II

**Functional Duties/Responsibilities:** Under minimal direction, provides advanced level understanding related to cybersecurity. Includes familiarity with the legal and regulatory privacy-related cybersecurity frameworks associated with respective critical infrastructure sectors, especially as related to common cybersecurity practices, assessment and testing methodologies,and cybersecurity tools and metrics. Applies subject matter expertise to high-level analysis, and guidance development for cybersecurity challenges.

**Education/Experience Required:** BS degree in Computer Science or a related field and eight (8) years of IT technical experience including at least five (5) years of experience in cybersecurity.

### Job Title: Cybersecurity Subject Matter Expert III

**Functional Duties/Responsibilities:** Provides expert level understanding related to cybersecurity, based on experience in one or more critical infrastructure sectors. Includes familiarity with the legal and regulatory cybersecurity frameworks associated with respective critical infrastructure sectors, especially as related to executive-level risk management, common cybersecurity practices, assessments, testing, and cybersecurity tools and metrics. Applies subject matter expertise to high-level analysis, and guides development for cybersecurity challenges. Applies high-level facilitation skills within large groups in order to derive stakeholder cybersecurity imperatives and support the prioritization of sometimes competing Digital Identity Management-related cybersecurity imperatives.

**Education/Experience Required:** BS degree in Computer Science or a related field and ten (10) years of IT technical experience including at least seven (7) years of experience in cybersecurity.

### Job Title: Cybersecurity Subject Matter Expert IV

**Functional Duties/Responsibilities:** Provides expert level understanding related to cybersecurity, based on experience in one or more critical infrastructure sectors. Includes familiarity with the legal and regulatory cybersecurity frameworks associated with respective critical infrastructure sectors, especially as related to executive-level risk management, common cybersecurity practices, and cybersecurity tools and metrics. Applies subject matter expertise to high-level analysis, and guides development for cybersecurity challenges. Applies high-level facilitation skills within large groups in order to derive stakeholder cybersecurity imperatives and support the prioritization of sometimes competing Digital Identity Management-related cybersecurity imperatives.

**Education/Experience Required:** BS degree in Computer Science or a related field and twelve (12) years of IT technical experience including at least nine (9) years of experience in cybersecurity.

### Job Title: Cybersecurity Project Manager

**Functional Duties/Responsibilities:** Manages, plans, schedules, communicates, facilitates, monitors, and controls cybersecurity project related tasks to ensure timely implementation of releases through deployment, and, in accordance with Project Management standards and procedures. Determines, monitors, and reviews all project economics to include costs, operational budgets, staffing requirements, sub-contractors, resources and risk. Plans, schedules, monitors, and reports on activities related to the project. Using Scrum methodologies, leads the project team(s) in determining client requirements and translating requirements into operational plans. Controls project requirements, scope, and change management issues. Coaches members of cross-functional teams to accomplish project goals, to meet established schedules, and resolve technical/operational issues. Establishes appropriate metrics for measuring key program criteria. These responsibilities include managing cross-functional teams, and delivering approved projects on time, within budget, and with quality results.

**Education/Experience Required:** A Bachelor's degree in computer science, information systems, business, engineering or related scientific or technical discipline. This position requires a minimum of two (2) years project management experience, one (1) of which must be as a project manager in a cybersecurity environment. Scrum experience or certification is desired.

### Job Title: Cybersecurity Program Manager

**Functional Duties/Responsibilities:** Plans, directs, and coordinates a cross-functional team's activities to manage and implement cybersecurity project and/or interrelated programs from contract initiation to final operational stage. Leads teams to develop plans that model program commitments and timing. Leads the project/program team(s) in determining client requirements and translating requirements into operational plans. Determines, monitors, and reviews all project/program economics to include costs, operational budgets, staffing requirements, resources and risk. Identifies and assembles the appropriate blend of resources to meet program needs and requirements; monitors and reports on activities related to the project/program. Meets with customers to review program scope/progress and resolve program issues. Controls project/program requirements, scope, and change management issues. Formulates contingency plans to address schedule revisions, risk, fund allocations, and work requirements. Ensures adherence to legally binding requirements and client's long-term strategic goals. Coaches members of cross-functional teams to accomplish project/program goals, to meet established schedules, and resolve technical/operational issues. Establishes appropriate metrics for measuring key program criteria. Maintains awareness of emerging technologies in security and digital identity management and project/program management techniques.

**Education/Experience Required:** A Bachelor's degree in computer science, information systems, business, engineering or related scientific or technical discipline. This position requires a minimum of six (6) years of IT experience including four (4) years cybersecurity or identity management related experience, and a minimum of four (4) years as a project manager. Experience includes increasing responsibilities in program and project management supporting cybersecurity or identity management related efforts. Scrum experience or certification is desired.

# ICAM PROFESSIONAL SERVICES RATES

# SIN 541519ICAM, SIN 541519ICAMSSTLOC

| SIN | Labor Category | 11/1/2022 – 2/19/22 | 2/20/23 - 2/19/24 |
|---|---|---|---|
| 541519ICAM | Senior Security and Digital Identity Management SME | $352.37 | $366.82 |
| 541519ICAM | Security and Digital Identity Management SME | $270.70 | $281.80 |
| 541519ICAM | Senior Security and Digital Identity Management Architect | $256.70 | $267.22 |
| 541519ICAM | Security and Digital Identity Management Architect | $243.15 | $253.12 |
| 541519ICAM | Security and Digital Identity Management Program Manager | $181.38 | $188.82 |
| 541519ICAM | Security and Digital Identity Management Project Manager | $155.56 | $161.93 |
| 541519ICAM | Security and Digital Identity Management Technical Specialist | $154.65 | $160.99 |
| 541519ICAM | Senior Identity Management Policy Analyst | $257.67 | $268.24 |
| 541519ICAM | Identity Management Policy Analyst | $132.85 | $138.30 |

## SIN 541519ICAM & 541519ICAMSTLOC
## Identity and Access Management Professional Services

**Job Title: Senior Security and Digital Identity Management SME**
**Functional Duties/Responsibilities:** Provides expert level understanding related to digital identity management and cybersecurity, based on experience in one or more critical infrastructure sectors. Includes familiarity with the legal and regulatory privacy-related cybersecurity frameworks associated with respective critical infrastructure sectors, especially as related to executive-level risk management, common cybersecurity practices, and cybersecurity tools and metrics. Applies subject matter expertise to high-level analysis, and guides development for cybersecurity challenges. Applies high-level facilitation skills within large groups in order to derive stakeholder cybersecurity imperatives and support the prioritization of sometimes competing Digital Identity Management-related cybersecurity imperatives.

**Education/Experience Required:** A Bachelor's degree in computer science, information systems, business, engineering or related scientific or technical discipline. Bachelor's Degree and twelve (12) years of technical experience with at least 8 years of experience with security and identity management technical solutions. Expert in Government security and identity management standards and has extensive domain expertise.

**Job Title: Security and Digital Identity Management SME**

**Functional Duties/Responsibilities:** Provides advanced level understanding related to digital identity management and cybersecurity, based on experience in one or more critical infrastructure sectors. Includes familiarity with the legal and regulatory privacy-related cybersecurity frameworks associated with respective critical infrastructure sectors, especially as related to executive-level risk management, common cybersecurity practices, and cybersecurity tools and metrics. Applies subject matter expertise to high-level analysis, and guidance development for cybersecurity challenges. Applies facilitation skills in order to derive stakeholder cybersecurity imperatives and support the prioritization of sometimes competing Digital Identity Management-related cybersecurity imperatives.

**Education/Experience Required:** A Bachelor's degree in computer science, information systems, business, engineering or related scientific or technical discipline. Bachelor's Degree and eight (8) years of technical experience with at least 6 years of experience with security and identity management technical solutions. Expert in Government security and identity management standards and has extensive domain expertise.

**Job Title: Senior Security and Digital Identity Management Architect**

**Functional Duties/Responsibilities:** Provides technical/management leadership on major tasks or technology assignments involving security and digital identity management operations. Partners with all aspects of the business/ business units (BUs) to help align business goals to technical architecture for the program. Partners with IT management to establish and institutionalize processes and procedures for security and digital identity management; leads the development and deployment activities; facilitates design reviews and code walkthroughs; organizes and participates in testing activities to ensure delivery of quality systems; prepares and manages project plans and milestones; estimates level of effort and resource utilization; anticipates and resolves issues and risks; ensures the projects are delivered with high quality; contributes to the development and continuous review of appropriate practices, standards and guidelines. Leads and directs a team of architects as part of a larger effort. Provide subject matter expertise on the various security and digital identity management applications.

**Education/Experience Required:** Bachelor's degree in Computer Science or related field and ten (10) years of technical experience including at least five (5) years of experience with architecture of security and identity management-based systems.

**Job Title: Security and Digital Identity Management Architect**

**Functional Duties/Responsibilities:** Under broad direction, collaborates with end-users to define, analyze and review business requirements for security and digital identity management projects. Collaborates with the technical team to define technical specifications and system design. Partners with the business/ business units (BUs) to help align business goals to technical architecture for the program. Partners with IT management to establish and institutionalize processes and procedures for security and digital identity management; supports the development and deployment activities; facilitates design reviews and code walkthroughs; supports and participates in testing activities to ensure delivery of quality systems; prepares and manages project plans and milestones; estimates level of effort and resource utilization; anticipates and resolves issues and risks; ensures the projects are delivered with high quality; contributes to the development and continuous review of appropriate practices, standards and guidelines. Supports a team of architects as part of a larger effort.

**Education/Experience Required:** Bachelor's degree in Computer Science or related field and seven (7) years of technical experience including at least four (4) years of experience with architecture of security and identity management-based systems.

**Job Title: Security and Digital Identity Management Program Manager**
**Functional Duties/Responsibilities:** Plans, directs, and coordinates a cross-functional team's activities to manage and implement project and/or interrelated programs from contract initiation to final operational stage. Leads teams to develop plans that model program commitments and timing. Leads the project/program team(s) in determining client requirements and translating requirements into operational plans. Determines, monitors, and reviews all project/program economics to include costs, operational budgets, staffing requirements, resources and risk. Identifies and assembles the appropriate blend of resources to meet program needs and requirements; monitors and reports on activities related to the project/program. Meets with customers to review program scope/progress and resolve program issues. Controls project/program requirements, scope, and change management issues. Works with senior management on program proposals, bids, contracts, estimates, and schedules. Formulates contingency plans to address schedule revisions, risk, fund allocations, and work requirements. Ensures adherence to legally binding requirements and client's long-term strategic goals. Coaches members of cross-functional teams to accomplish project/program goals, to meet established schedules, and resolve technical/operational issues. Establishes appropriate metrics for measuring key program criteria. Maintains awareness of emerging technologies in security and digital identity management and project/program management techniques.

**Education/Experience Required:** A Bachelor's degree in computer science, information systems, business, engineering or related scientific or technical discipline. This position requires a minimum of six (6) years of IT experience including four (4) years security or identity management related experience, and a minimum of four (4) years as a project manager. Experience includes increasing responsibilities in program and project management supporting security and identity management efforts. Scrum experience or certification is desired.

**Job Title: Security and Digital Identity Management Project Manager**
**Functional Duties/Responsibilities:** Manages, plans, schedules, communicates, facilitates, monitors, and controls project related tasks to ensure timely implementation of releases through deployment, and, in accordance with Project Management standards and procedures. Determines, monitors, and reviews all project economics to include costs, operational budgets, staffing requirements, sub-contractors, resources and risk. Plans, schedules, monitors, and reports on activities related to the project. Using Scrum methodologies, leads the project team(s) in determining client requirements and translating requirements into operational plans. Controls project requirements, scope, and change management issues. Coaches members of cross-functional teams to accomplish project goals, to meet established schedules, and resolve technical/operational issues. Establishes appropriate metrics for measuring key program criteria. These responsibilities include managing cross-functional teams, and delivering approved projects on time, within budget, and with quality results.

**Education/Experience Required:** A Bachelor's degree in computer science, information systems, business, engineering or related scientific or technical discipline. This position requires a minimum of two (2) years project management experience, one (1) of which must be as a project manager supporting security and identity management efforts. Scrum experience or certification is desired.

**Job Title: Security and Digital Identity Management Technical Specialist**

**Functional Duties/Responsibilities:** Under general direction, responsible for the technical implementation of the assigned security and identity management solution, according to the relevant customer's specification and the current requirements. Works with technical leadership to define requirements and the design for the security and identity management solution; ensures designs achieve high availability, maintainability and reliability of the product. Formulates and defines system scope and objectives, develops and modifies processes to solve issues for identity management systems to achieve desired results.

**Education/Experience Required:** A Bachelor's degree in computer science, information systems, business, engineering or related scientific or technical discipline. This position requires a minimum of two (2) years technical experience. Security and identity management experience is desired.

**Job Title: Senior Identity Management Policy Analyst**

**Functional Duties/Responsibilities:** Provides expert insight and analysis of policy issues resulting in recommendations for and/or drafts of major policy papers, positions, and other artifacts. Guides policy through all necessary review and approval processes. Provides subject matter expertise on advanced Identity & Access Management solutions, throughout all project and system lifecycle phases. Supports customer requirements gathering, product evaluations, and product integration.

**Education/Experience Required:** A Bachelor's degree in computer science, information systems, business, engineering or related scientific or technical discipline, to include strong policy coursework or degree. Bachelor's Degree and ten (10) years of technical experience with at least 8 years of experience with security and identity management policy solutions. Expert in Government security and identity management standards and has extensive domain expertise.

**Job Title: Identity Management Policy Analyst**

**Functional Duties/Responsibilities:** Under general direction, provides insight and analysis of policy issues. Supports the creation of policy documentation and artifacts. Assists with applying subject matter expertise on Identity & Access Management solutions, throughout all project and system lifecycle phases. Supports customer requirements gathering, product evaluations, and product integration.

**Education/Experience Required:** A Bachelor's degree in computer science, information systems, business, engineering or related scientific or technical discipline, to include policy coursework or degree. This position requires a minimum of two (2) years identity management-related experience.

**Education/Experience Substitution Table**

| DEGREE | DEGREE AND EXPERIENCE SUBSTITUTION | RELATED EXPERIENCE SUBSTITUTION |
|---|---|---|
| **Associate's** | **2 Years** | **2 Years** |
| **Bachelor's** | **Associate's + 2 Years** | **4 Years** |
| **Master's** | **Bachelor's + 2 Years** | **6 Years** |
| **Doctorate** | **Master's + 2 Years** | **8 Years** |