

LEGISLATIVE TRACKING FORM

Filing for Council Meeting Date: 04/21/26

Resolution Ordinance

Contact/Prepared By: _____

Date Prepared: _____

Title (Caption): A resolution accepting the terms of a cooperative purchasing master agreement with For The Record, Ltd.

for courtroom audio and visual equipment, service and storage for the State Trial Courts.

Submitted to Planning Commission? N/A Yes-Date: _____ Proposal No: _____

Proposing Department: _____ Requested By: _____

Affected Department(s): _____ Affected Council District(s): _____

Legislative Category (check one):

- | | | |
|---|--|--|
| <input type="checkbox"/> Bonds | <input type="checkbox"/> Contract Approval | <input type="checkbox"/> Intergovernmental Agreement |
| <input type="checkbox"/> Budget - Pay Plan | <input type="checkbox"/> Donation | <input type="checkbox"/> Lease |
| <input type="checkbox"/> Budget - 4% | <input type="checkbox"/> Easement Abandonment | <input type="checkbox"/> Maps |
| <input type="checkbox"/> Capital Improvements | <input type="checkbox"/> Easement Accept/Acquisition | <input type="checkbox"/> Master List A&E |
| <input type="checkbox"/> Capital Outlay Notes | <input type="checkbox"/> Grant | <input type="checkbox"/> Settlement of Claims/Lawsuits |
| <input type="checkbox"/> Code Amendment | <input type="checkbox"/> Grant Application | <input type="checkbox"/> Street/Highway Improvements |
| <input type="checkbox"/> Condemnation | <input type="checkbox"/> Improvement Acc. | <input type="checkbox"/> Other: _____ |

FINANCE Amount +/-: \$ _____ Funding Source: Capital Improvement Budget Capital Outlay Notes Departmental/Agency Budget Funds to Metro General Obligation Bonds Grant Increased Revenue Sources	Match: \$ _____ Judgments and Losses Local Government Investment Project Revenue Bonds Self-Insured Liability Solid Waste Reserve Unappropriated Fund Balance 4% Fund Other: _____
Approved by OMB: <u>José Nuñez</u> Approved by Finance/Accounts: _____ Approved by Div Grants Coordination: _____	Date to Finance Director's Office: <u>4/10/2026 10:22 AM CDT</u> APPROVED BY FINANCE DIRECTOR'S OFFICE: <u>Jennifer Reed/mjw</u>

ADMINISTRATION	
Council District Member Sponsors:	_____
Council Committee Chair Sponsors:	_____
Approved by Administration:	_____ Date: _____

DEPARTMENT OF LAW	
Date to Dept. of Law: _____	Approved by Department of Law: _____
Settlement Resolution/Memorandum Approved by: _____	
Date to Council: _____	For Council Meeting: _____ <input type="checkbox"/> E-mailed Clerk
<input type="checkbox"/> All Dept. Signatures <input type="checkbox"/> Copies <input type="checkbox"/> Backing <input type="checkbox"/> Legislative Summary <input type="checkbox"/> Settlement Memo <input type="checkbox"/> Clerk Letter <input type="checkbox"/> Ready to File	

Resolution No. _____

A resolution accepting the terms of a cooperative purchasing master agreement with For The Record, Ltd. for courtroom audio and visual equipment, service and storage for the State Trial Courts.

WHEREAS, Tennessee Code Annotated § 12-3-1205(b) allows the Metropolitan Government of Nashville and Davidson County ("Metro") to participate in a cooperative purchasing agreement for the procurement of any goods, supplies, services, or equipment with an agency of the United States; and,

WHEREAS, Tennessee Code Annotated § 12-3-1205(b) allows Metro to participate in a master agreement with an agency of the United States by adopting a resolution accepting the terms of the master agreement; and,

WHEREAS, the Purchasing Agent desires to participate in the master agreement between For The Record, Ltd. and the United States General Services Administration, a copy of which is attached hereto and incorporated herein; and,

WHEREAS, this master agreement was requested by the State Trial Courts but is available to all Metro Departments to utilize; and,

WHEREAS, Metro's participation in this out-of-state master agreement is limited to a term that will not exceed sixty months; and,

WHEREAS, approval of the master agreement is in the best interest of the citizens of Metropolitan Government of Nashville and Davidson County.

NOW, THEREFORE, BE IT RESOLVED BY THE COUNCIL OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY:

Section 1. That the master agreement between For The Record, Ltd. and the United States General Services Administration, a copy of which is attached hereto and incorporated herein, is hereby approved.

Section 2. That this resolution shall take effect from and after its adoption, the welfare of The Metropolitan Government of Nashville and Davidson County requiring it.

RECOMMENDED BY:

Dennis Rowland

Dennis Rowland
Purchasing Agent

INTRODUCED BY:

APPROVED AS TO AVAILABILITY
OF FUNDS:

Jenneen Reed/mjr

Jenneen Reed, Director
Department of Finance

Member(s) of Council

APPROVED AS TO FORM AND
LEGALITY:

Kelli Woodward

Assistant Metropolitan Attorney



Cooperative Request Form

Request Utilization of a Federal, Statewide, Municipal, or Cooperative Contract

A cooperative is when Metro utilizes a contract from another public entity to make a purchase. With the exception of statewide contracts, use of a cooperative requires Metro Council approval.

Cooperatives are not negotiable. Departments must accept the terms of the master contract without exception.

Questions? Email zak.kelley@nashville.gov.

Departmental Information

What is your name? Tammy Hawkins

What is your department? State Trial Courts

What is your email address? tammyhawkins@jisnashville.gov

What is your phone number? (615) 880-2558

In addition to your department, will other Metro departments be utilizing this cooperative? No.

How much do you estimate spending on this cooperative contract? \$3,600,000.00

Cooperative Information

What is the cooperative entity? Federal government.

What is the lead agency? US Government

Who is the supplier? FTR, LTD (For The Record)

Is the supplier registered in iSupplier? No.

What is the contract number? 47QTCA24D001Q

When did the contract start? Tuesday, November 14, 2023

When does the contract end? Monday, November 13, 2028

What was the solicitation method for this contract?

Other.

What is the good/service that this cooperative will be utilized to purchase?

Courtroom Audio/Video equipment, service and storage.

Why is utilizing this cooperative contract more advantageous to Metro than issuing our own RFP/ITB?

The existing equipment is over 10 years old and replacement is time-sensitive; using a current contract helps avoid delays that could lead to operational disruptions or increased maintenance costs. A current contract has already gone through the competitive bid and compliance process, allowing the organization to move forward quickly without repeating lengthy procurement steps.

Upload the original contract from the lead agency.



0ZZSB9.3VQ55X_47QTCA24D001Q_F... .pdf

Does the contract contain any good/service relative to surveillance as described in MCL 13.08.080?

No.

This contract contains a cooperative purchase provision that allows use by other governmental agencies and/or use of this contract is authorized by state and local law.

Yes.

I accept the terms of this contract without exception.

Yes.

Upload the formal solicitation (RFP/ITB) from the lead agency.



Information Technology_Category_Att... .pdf

This solicitation was advertised, open, and unrestricted.

Yes.

I have confirmed with both my department finance manager and/or OMB budget analyst sufficient fund availability for this request.

Yes

I affirm that I am authorized by the appropriate individuals in my department, including my director or their designee, to submit this cooperative request.

Yes



Cooperative Request Review – Federal Contract

This cooperative request for **courtroom audio/visual equipment, service and storage from For the Record via federal general service administration (GSA) contract 47QTCA24D001Q** is recommended for approval.

The anticipated project value is **\$3,600,000.00**. The cooperative will be utilized by **State Trial Courts**.

Council approval is required per TCA 12-3-1201.

Legal Justification

T.C.A. § 12-3-1201 (c) & MCL 4.12.090 (b) authorize Metro to purchase goods, supplies, services, and equipment under the provision of contracts or price agreements of open federal contracts.

Contract 47QTCA24D001Q meets this standard.

Regulatory Justification

R4.12.090.02 of the regulations to the procurement authorizes Metro to purchase goods or services from intergovernmental cooperative purchasing agreements, provided that the contracts are reviewed for price and opportunity cost.

Based on information provided by the department, contract 47QTCA24D001Q meets this standard.

Value Justification

It is unlikely that Metro, as a single government entity, would obtain better value through a competitive solicitation. That is because the pricing in this GSA contract leverages the scale of federal government.

Impact on Minority & Women Owned Businesses

Pursuant to R4.12.090.05 of the regulations to the procurement code, Metro will work with the cooperative entity to maximize participation of disadvantaged firms in accordance with MCL 4.44 and 4.46.

Prepared by Kristin Butler
3/30/2026



Cooperative Request Signature Form

Co-Op Request Number	C2026089
Date Received	March 23, 2026

To Whom It May Concern,

I have read the attached Cooperative Review and concur with the recommendation contained therein.

Should you have questions, please contact the reviewer or reach out to me directly.

Regards,

Dennis Rowland

DR

3/30/2026 | 1:01 PM CDT

Dennis Rowland
Purchasing Agent & Chief Procurement Officer

Date Signed



Category Attachment

Code : **F**

Title : **Information Technology**

Solicitation Number : **47QSMD20R0001**

Refresh Number : **0030**

Created on November 24, 2025

Information Technology Category Instructions and Regulations

Instructions:

All offerors must follow evaluation criteria and instructions outlined in the MAS solicitation, including in SCP-FSS-001. The Information Technology category attachment outlines additional evaluation criteria, requirements, and information specific to this category only. For a list of required MAS templates and attachments, please visit the [Required templates for a MAS offer](#) page. For category specific attachments and templates, please visit the [Multiple Award Schedule](#) page (the table located in the middle of the homepage provides the required additional attachments by large category).

For additional guidance and information for Schedule buyers and sellers, please visit our general guidance page at [Multiple Award Schedule](#) page.

General Information

Executive Order on Defending Women from gender ideology extremism and restoring biological truth to the federal government: In accordance with sections 3(e) and (g) of Executive Order 14168, "[Defending Women from gender ideology extremism and restoring biological truth to the federal government](#)" dated January 20, 2025, "[a]gencies shall take all necessary steps, as permitted by law, to end the Federal funding of gender ideology" and "Federal funds shall not be used to promote gender ideology." Any products, services, or solutions that violate the aforementioned provisions of the Executive Order are excluded from the scope of the MAS program.

Executive Order on Initial Rescissions of Harmful Executive Orders and Actions: In light of [E.O. 14148](#), [Initial Rescissions of Harmful Executive Orders and Actions](#), dated January 20, 2025, which revokes, among others, [E.O. 14057](#), [Catalyzing Clean Energy Industries and Jobs Through Federal Sustainability](#), the MAS program is removing all references to non-statutory sustainability requirements, programs, and preferences from its SIN instructions and descriptions.

Executive Order on Ending Procurement and Forced use of Paper Straws: In accordance with Section 2 of [E.O. 14208](#), [Ending Procurement and Forced Use of Paper Straws](#), dated February 10, 2025, "[a]gencies shall take all appropriate action to eliminate the procurement of paper straws and otherwise ensure that paper straws are no longer provided within agency buildings." Any products, services, or solutions that violate the aforementioned provisions of the Executive Order are excluded from the scope of the MAS program.

Discontinuation of Offerings Based on Revoked Climate-related Executive Orders: In accordance with Section 4(e) of [E.O. 14154](#), [E.O. 14148](#), and [E.O. 14236](#), products or services associated with revoked E.O.'s (e.g., [E.O. 14057](#), [E.O. 13990](#), and [E.O. 14096](#)) that do not have a statutory basis are excluded from the scope of the MAS program. This includes offerings related to the social cost of greenhouse gas emissions, social governance, environmental justice, and corporate social responsibility. Products and services supported by statutory authority remain within the scope of the MAS program.

Executive Order on Ending Radical and Wasteful Government DEI Programs: In accordance with [E.O. 14151](#), [Ending Radical and Wasteful Government DEI Programs and Preferencing](#), dated January 20, 2025, [E.O. 14173](#), [Ending Illegal Discrimination And Restoring Merit-Based Opportunity](#), dated January 21, 2025, and [Fact Sheet: President Donald J. Trump Protects Civil Rights and Merit-Based Opportunity by Ending Illegal DEI](#), dated January 22, 2025, which "terminates "diversity, equity, and inclusion" (DEI) discrimination in the federal workforce, and in federal contracting and spending", any products, services, or solutions that violate the aforementioned provisions of the Executive Order are excluded from the scope of the MAS program.

Guidance on Payment for Software Licenses Delivered via Software as a Service (SaaS):

Background: SaaS is a cloud-based method of software delivery and licensing in which software is accessed online, commonly on a subscription basis. The purchaser receives access to the license contemporaneously with payment by downloading or accessing the software (and updates) via internet (web) based platforms. The purchased software license typically comes with a software license term that reflects the time period in which the license will grant users access to the software via SaaS delivery.

In the context of software licenses delivered or accessed via SaaS, payment is often made "upfront," meaning that payment is made contemporaneously with receipt of the software license and the beginning of the license service term. GSA has considered whether such upfront payment is considered an advance payment. As

explained below, it is not.

Advance payment is a specific type of contract financing method where payments are made prior to delivery or completion of the product or a service. There are statutory limitations (*e.g.*, 31 U.S.C. § 3324 and 41 U.S.C. § 4505) on the Federal Government's use of advance payments. Advance payments to Government contractors for goods and services are generally prohibited unless specifically authorized. Advance payment is not authorized for the purchase of software licenses delivered or accessed via SaaS.

For purchases meeting the criteria described below, upfront payment for software licenses delivered or accessed via SaaS is not considered advance payment. The central distinction is the contemporaneous access.

Criteria: Upfront payment for software licenses delivered or accessed via SaaS is not considered advance payment. The central distinction is the contemporaneous access as long as the purchase meets the following criteria:

- Access to the software is granted contemporaneously with payment (i.e., delivery of the license is made contemporaneously with payment);
- The license is acquired on a fixed-price or fixed-price with economic price adjustment basis even if other portions of the task order or contract are not fixed price;
- The license is priced at a single seat, multi-seat, unit, or subscription price covering a fixed term, defined as "a limited period of time";
- The license's pricing/billing model allows for no utilization or consumption metric other than quantity to affect the costs incurred over the negotiated term;
- The license does not require any upfront payment other than the fixed seat, unit, or subscription cost as a prerequisite for access or a pricing discount; and
- Within end user or other license agreements, the license service is continuous and uninterrupted for the negotiated term of access to the license.

All other cloud computing services (*i.e.*, *IaaS*, *PaaS*, *SaaS*) and professional services must be paid in arrears in accordance with 31 U.S.C. § 3324 and 41 U.S.C. § 4505.

Drones/Unmanned Aircraft Systems: GSA will not award any Drones/Unmanned Aircraft Systems (UAS), as defined in 49 USC Ch. 448, in response to this Solicitation except those drones approved by the Department of Defense (DoD) Defense Innovation Unit (DIU) through its Blue sUAS Program.

**FAR 52.240-91(c) further prohibits delivering any FASC - prohibited unmanned aircraft system, which includes unmanned aircraft (i.e., drones) and associated elements (i.e., the equipment required for control and operation, such as communication links and the software or systems necessary for their safe and effective functioning). On or after December 22, 2025, Contractors are prohibited from operating or using Federal funds to procure or operate a FASC-prohibited unmanned aircraft system.

Firearms and Ammunition: GSA will not award weapons such as firearms, live ammunition, explosives, and artillery weapons under this Solicitation. This also includes components that are solely used to produce functional weapons. Components that will not be awarded under this Solicitation include, but are not limited to, barrels, chambers, bolts, trigger groups, stock, magazines, rockets, grenades, grenade launchers, mines and mortars, cases, primers, powder, and projectiles.

This exclusion does not apply to non-lethal ammunition types intended to be used for training, safety, and marking purposes.

CONUS/OCONUS Requirements: Some requirements may apply only to applications in the Continental United States (CONUS), Alaska, Hawaii and Puerto Rico. For products and services proposed internationally (OCONUS), the commensurate standards will apply and should be provided with the offer but will be reviewed by the ordering activity for compliance with the local requirements and standards.

General Out of Scope Items: GSA will not award items that fall under the following categories:

- Remanufactured (except toner)
- Automotive parts
- Personal hygiene items
- Fully assembled fixed-wing aircraft
- Books and publications (except technical publications and reports on SIN 511120)
- Children's toys, dolls and games
- Promotional products
- Sporting goods
- General clothing items (except workwear under SIN 3152, uniforms under SIN 315210 and protective apparel under SIN 339113PA)

- Swimming pool equipment and supplies
- Musical instruments
- Customizable awards, medals and ribbons

AI/ML Model Training Restrictions: The use of Government data for the purpose of training Artificial Intelligence/Machine Learning (AI/ML) models and systems is prohibited without explicit written authorization from the ordering activity contracting officer.

Definition: Government data means any information, (including metadata), document, media, or machine-readable material regardless of physical form or characteristics that is created or obtained by the Government, or a contractor on behalf of the Government, in the course of official Government business.

Section I Instructions for all IT Offerors:

1) **Technical Evaluation.** All technical evaluation factors, subcategory and SIN specific requirements will be reviewed, evaluated, and rated acceptable or unacceptable based on criteria defined in the solicitation. Award will be made on a SIN-by-SIN basis. A rating of "unacceptable" under any technical evaluation factor by SIN will result in an "unacceptable" rating overall for that SIN, and that SIN will be rejected. Offers determined unacceptable for all proposed SIN(s) will be rejected.

2) **Commercial Supplier Agreement (CSA) Terms.** If offering Commercial Supplier Agreement (CSA) Terms (e.g. standard terms of sales or lease, Terms of Service (TOS), End User License Agreements (EULA), or other similar legal instruments or agreements) - Often ordering activities will decline to place an order because of Federally non-compliant terms (e.g., customer indemnification). This results in a loss of business for the Schedule holder. In order to facilitate GSA's review and negotiation of each individual set of terms for compliance with Federal law, the Offeror is required to submit its CSA in an editable format, and preferably with the Federally non-compliant terms and conditions already removed. Such submissions may help GSA avoid delays in reviewing and negotiating each individual agreement. "Clickwrap" submissions or links to agreements are not acceptable. The Offeror must clearly define what additional products, services, and prices are included with its CSA.

3) **Part Numbers.** Offeror must ensure the Original Equipment Manufacturer (OEM), Manufacturer Part Number or Wholesaler Number for each product proposed reflects the actual part number assigned. If the OEM, Manufacturer, or Wholesaler Part Number is submitted incorrectly or not submitted, the product offering will not be awarded.

4) **Ancillary Supplies and/or Services.**

- a) Ancillary products and services are not within the scope of any ITC SIN and must be offered under a SIN that specifically covers the proposed products and services.
- b) Non-professional labor categories must be incidental to and used solely to support hardware, software and/or professional services, and cannot be purchased separately. Non-professional labor categories must be offered under a SIN that specifically covers the proposed services.

5) **Relevant Project Experience Evaluation.**

- a) The Offeror must submit a narrative demonstrating relevant project experience. A narrative is required for the following SINs:

Cloud Services Subcategory

- 518210C - Cloud Computing and Cloud Related IT Professional Services

Financial Management Services Subcategory

- 518210FM – Financial Management Quality Service Management Office (FM QSMO) Core Financial Management (FM) Solutions and IT Professional Services

IT Services Subcategory

- 54151HACS - Highly Adaptive Cybersecurity Services (HACS)
- 54151S - Information Technology Professional Services
- 54151HEAL - Health Information Technology Services

IT Solutions Subcategory

- 561422 - Automated Contact Center Solutions (ACCS)
- 541370GEO - Earth Observation Solutions
- 541519ICAM - Identity, Credentialing and Access Management (ICAM)
- 541519PIV - Homeland Security Presidential Directive 12 Product and Service Components
- 541519PKI - Public Key Infrastructure (PKI) Shared Service Providers (PKI SSP) Program
- 541519CSP – Credential Service Providers (CSP)

Telecommunications Subcategory

- 517312 - Wireless Mobility Solutions
- 517410 - Commercial Satellite Communications Solutions (COMSATCOM)

IT Training Subcategory

- 611420 – Information Technology Training

In addition to the one (1) relevant project experience submission required by the SCP-FSS-001 Factor Four, Information Technology Category (ITC) **requires one (1) additional project experience for the SINs listed above. This equates to a total of two (2) project experiences with your offer submission.** Relevant projects must be within the last two years and not exceed four (4) pages per project. Each description must clearly indicate the SIN to which it applies, and identify the specific services being proposed under that SIN. The two (2) projects can be completed or on-going project(s), similar in size and complexity to the effort contemplated herein and in sufficient detail for the Government to perform an evaluation.

i. Each project description must also address the following elements:

1. Provide the following information for each project submitted:

A. Project/Contract Name;

B. Project Description;

C. Dollar Amount of Contract;

D. Project Duration, which includes the original estimated completion date and the actual completion date; and

E. Point of Contact and Telephone Number.

ii. Detailed description of SIN-relevant work performed and results achieved.

iii. Provide background information on the project or projects presented to demonstrate expertise.

iv. Methodology, tools, and/or processes utilized in performing the work.

v. Demonstration of compliance with any applicable laws, regulations, Executive Orders, OMB Circulars, professional standards, etc.

vi. Project schedule (i.e., major milestones, tasks, deliverables), including an explanation of any delays.

vii. How the work performed is similar in scope and complexity to the work solicited under the proposed SIN.

viii. Demonstration of required specific experience and/or special qualifications detailed under the proposed SIN.

ix. Submit a summary of the final deliverables for the noted project or projects.

x. The Offeror may use the same project in support of more than one SIN as long as the description clearly identifies the SIN-relevant work. All examples of completed services must have been deemed acceptable by the customer.

xi. All examples of completed services shall have been found to be acceptable by the ordering activity. If the offeror cannot provide two examples of past experience, they may provide additional documentation to substantiate project experience to be evaluated by the contracting officer.

b) The following SINs have additional requirements that shall be addressed in the Relevant Project experience narrative:

i. SIN 54151HEAL - Health Information Technology Services:

1. Each completed example of project experience shall have been completed within the last two years. All examples of completed services shall have been found to be acceptable by the ordering activity.

2. Provide background information on the project or projects presented to demonstrate Health IT expertise.

3. Outline how the project or projects are related to SIN 54151HEAL.

ii. SIN 561422 - Automated Contact Center Solutions (ACCS)

1. Where applicable include descriptions of types of channels used in contact centers, annual volume of contacts by channel, Customer Relationship Management tools, speech and text analytics tools used, summary of employee engagement/retention practices used, multilingual services, summary of any efforts or practices used to support surge volume, list of accomplishments to include improvements in service, numbers of agents (including actual, virtual/home-based or Artificial Intelligence/Natural Language/Intelligence Language) used in the project, security considerations, summary of PII handling practices, and types of reporting/data analytics provided on the project.

iii. SIN 541370GEO - Earth Observation Solutions

1. A narrative of services provided or a project where products were provided.

iv. SIN 541519ICAM - Identity, Credentialing and Access Management (ICAM)

1. Both projects described must be prior Federal Government application deployment projects for public-facing IT systems.

2. Technical evaluation criteria for offers of policy-compliant agency setup, testing, identity proofing, credential issuance, subscriber customer service account management, revocation, and credential validation as part of the basic service.

A. Successful completion of Level 1 Credential Assessment - Include Assessment Report

B. Successful completion of Level 2 Credential Assessment - Include Assessment Report

C. Successful completion of applicable interoperability testing - Include Test Report

3. Technical evaluation criteria for offers of compliant ID proofing, Credential issuance, continued account management, revocation, and certificate validation as part of the basic service.

A. Successful completion of Level 3 and 4 Credential Assessment - Include Assessment Report

B. Access Certificates for Electronic Services (ACES) Security Certification and Accreditation (C&A) as a condition of obtaining and retaining approval to operate as a Certification Authority (CA) under the ACES Certificate policy and the GSA ACES Program. – Include Authorization to Operate (ATO) letter.

C. Common criteria for other Certification Authorities cross-certified by the Federal Bridge

4. Technical evaluation criteria for offers of E-authentication Hardware Tokens.

A. Listed on GSA's Federal Information Processing Standards (FIPS) 201 Approved Products List.

B. Crypto Modules must be FIPS 140-2 validated.

5. Technical evaluation criteria for offers of precursor services such as bulk load, testing, identity proofing, credential issuance, subscriber customer service account management, revocation, and credential validation as part of the basic service. Also includes translation and validation services, and partial services such as 3rd-party identity proofing or secure hosting.

A. Demonstrated compliance with NIST SP 800-63, as applicable to the technologies being utilized by the offeror.

B. Compliance with published E-Authentication architecture, verified by a clearance letter from GSA's Office of Governmentwide Policy.

6. Technical evaluation criteria for offers of Identity and Access Management Professional Services.

A. Documented experience with deployment of policy-compliant Identity and Access Management (IAM) projects in Government agencies. This includes IAM technologies and standards, including Security Assertion Markup Language (SAML), Public Key Infrastructure (PKI) and the Web Services (WS)-Federation specification. Offerors should describe in detail their competencies when proposing under this SIN.

v. SIN 541519PIV - Homeland Security Presidential Directive 12 Product and Service Components

1. All offers must be in compliance with guidance in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, OMB Memorandum 04-04.

vi. SIN 517410 - Commercial Satellite Communications Solutions (COMSATCOM)

1. Provide a description of the offeror's experience delivering COMSATCOM services as described in 552.238-110 Commercial Satellite Communication (COMSATCOM) Services.

2. All completed projects shall have been completed within the last two years prior to submission of the COMSATCOM SIN proposal.

3. If the offeror cannot provide two (2) projects, it may provide additional documentation to substantiate project experience to be evaluated by the contracting officer.

4. Provide background information on the project presented to demonstrate familiarity and expertise servicing COMSATCOM requirements.

5. Outline how the project is related to the COMSATCOM SIN.

6. Information Assurance Minimum Security Controls Compliance for SIN 517410 COMSATCOM

A. Federal policy specifies Government customer compliance with the Federal Information Security Management Act of 2002, as implemented by Federal Information Processing Standards Publication 200 (FIPS 200), "Minimum Security Requirements for Federal Information and Information Systems." This standard specifies minimum security requirements Federal agencies must meet, defined through the use of security controls described in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," DoD Instruction (DoDI) 8500.2, "Information Assurance Implementation," and associated documents.

B. Complete the Information Assurance Checklist found on the [SIN 517410 Satellite](#)

[Communications Resources](#) page.

C. The Government will evaluate the Information Assurance checklist submitted as part of offeror's proposal to determine whether the offeror understands the minimum-security controls, and has processes, personnel, and infrastructure that currently complies or demonstrates a reasonable approach to becoming compliant with all the minimum security controls for at least a low-impact information system or MAC III system.

vii. **SIN 611420 – Information Technology Training**

1. The narrative must include the following:

- A. course names,
- B. brief description,
- C. length of course,
- D. type of training,
- E. location (on or off customer site), and
- F. any other pertinent details to the training offered.

2. If other than the manufacturer, submit proof of authorization to provide training course(s) for manufacturer's software and/or hardware products.

6) SINS with IT Professional Services. This applies to all SINS that include IT professional services, the offeror shall not resell IT professional services. Currently, the IT Services subcategory and the IT Solutions subcategory include SINS with IT professional services.

This applies to all SINS that include IT professional services, the offeror shall not provide services which fall under the Brooks Act. FAR 36.6, which distinguishes between mapping services of an A/E nature and mapping services which are not connected nor incidental to the traditionally accepted A/E Services.

7) Cooperative Purchasing. Section 211 of the E-Government Act of 2002 amended the Federal Property and Administrative Services Act to allow for cooperative purchasing. Cooperative Purchasing authorizes State and local government entities to purchase Information Technology (IT) supplies/products and services from MAS Contracts that include SINS from IT Category of the MAS Consolidated Solicitation.

8) IT Hardware Shipped FOB Destination. Prices for equipment shall be FOB destination, which covers equipment delivery to destination for any location within the geographic scope of this contract. This applies to all SINS offering hardware.

IT Hardware Subcategory

- 33411 - Purchasing of New Electronic Equipment

9) Internet Protocol Version 6 (IPv6). All Information Technology offers at the time of submission dealing with Internet Protocol (IP) are self-certifying offerings as Internet Protocol Version 6 (IPv6) compliant.

10) Payment Under a Contract. Charges for training, maintenance, and services must be billed and paid in arrears (31 U.S.C. 3324).

11) Continuous Diagnostics and Mitigation (CDM) Approved Products. GSA has partnered with the Cybersecurity and Infrastructure Security Agency (CISA) to showcase CISA approved CDM tools. The CISA CDM Program's Approved Products List (APL) is the authoritative catalog for all approved CDM Tools and associated services. CDM APL Tools will carry the [CDM](#) tools symbol. The full complement of CDM subcategories includes tools, associated maintenance, and other related activities such as training. The CDM products and associated services undergo a DHS CISA product qualification process in order to be added to the CDM Approved Products List (APL). The APL features high-quality cybersecurity vendors offering products and related services to Federal, State, and Local Governments. CISA only accepts submissions to modify the CDM APL monthly. Offerors can submit updates to the APL on the first Monday of the first full or partial week of the month, with submissions being accepted through Friday of that week. A full submission calendar can be found on the CISA

[website](#). For technical and CDM APL related questions, please contact the CISA CDM Program Office at (csd_cb.acqbudg@cisa.dhs.gov).

Section II Terms and Conditions for all IT Contractors

1) Organizational Conflicts Of Interest

a) Definitions.

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

"Contractor and its affiliates" and "Contractor or its affiliates" refers to the Contractor, its chief executives, directors, officers, subsidiaries, affiliates, subcontractors at any tier, and consultants and any joint venture involving the Contractor, any entity into or with which the Contractor subsequently merges or affiliates, or any other successor or assignee of the Contractor.

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

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

2) Services Performed

a) All 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.

3) **Travel.** Any Contractor travel required in the performance of 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.

4) Warranty

a) Unless otherwise specified in the contract, the Contractor's standard commercial warranty applies.

b) The Contractor's commercial guarantee/warranty shall be included in the Commercial Supplier Agreement 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.

Regulation Number	Regulation Title/Comments
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) (DEVIATION - NOV 2025)
52.229-1	STATE AND LOCAL TAXES (APR 1984)
552.238-107	TRAFFIC RELEASE (SUPPLIES) (MAY 2019)
552.238-73	IDENTIFICATION OF ELECTRONIC OFFICE EQUIPMENT PROVIDING ACCESSIBILITY FOR INDIVIDUALS WITH DISABILITIES (MAR 2022)
552.238-89	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)

Subcategory Instructions and Regulations

F01. Cloud Services Subcategory

Instructions:

Offerors submitting an offer for a SIN(s) under the “Cloud Services Subcategory” must also comply with the following:

1. The following applies to the Cloud Services SIN that includes Cloud Related IT Professional Services.

- a. Only Cloud Related IT Professional Services or Labor Categories shall be offered
- b. Offerors shall provide résumés to the GSA contracting officer or the user ordering activity upon request.
- c. Offerors shall provide a description of each type of Cloud Related IT Professional Service or Labor Category offered, and it should be presented in the same manner as the Contractor sells to its commercial customers. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles (labor categories) for those individuals who will perform the service must be provided.

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

EXAMPLE: Commercial Job Title: Cloud System Engineer

Minimum/General Experience: Three (3) years of technical experience which applies to cloud systems analysis and design techniques for complex computer systems. Requires competence in all phases of systems analysis techniques, concepts, and methods; also requires knowledge of available hardware, system software, input/output devices, structure, and management practices.

Functional Responsibility: Guides users in formulating requirements, advises alternative approaches, and conducts feasibility studies.

- d. Pricing for each type of Cloud Related IT Professional Service or Labor Category shall be in accordance with customary commercial practices; e.g., hourly rates, monthly rates, term rates, and/or fixed prices, minimum general experience, and minimum education.
- e. Pricing of services shall be offered at the Contractor’s facility and/or at the ordering activity location in accordance with customary commercial practices.
- f. All awarded professional services/labor categories shall be included as an attachment to the GSA Price List (I-FSS-600 CONTRACT PRICE LISTS (see current Solicitation for clause effective date)) in the format provided above.

2. **Continuous Diagnostics and Mitigation (CDM) Approved Products** - GSA has partnered with the Cybersecurity and Infrastructure Security Agency (CISA) to showcase CISA approved CDM tools. The

CISA CDM Program’s Approved Products List (APL) is the authoritative catalog for all approved CDM Tools and associated services. CDM APL Tools will carry the [CDM](#) tools symbol. The full complement of CDM subcategories includes tools, associated maintenance, and other related activities such as training. The CDM products and associated services undergo a DHS CISA product qualification process in order to be added to the CDM Approved Products List (APL). The APL features high-quality cybersecurity vendors offering products and related services to Federal, State, and Local Governments. CISA only accepts submissions to modify the CDM APL monthly. Offerors can submit updates to the APL on the first Monday of the first full or partial week of the month, with submissions being accepted through Friday of that week. A full submission calendar can be found on the CISA [website](#). For technical and CDM APL related questions, please contact the CISA CDM Program Office at (csd_cb.acqbudg@cisa.dhs.gov).

SIN 518210C Cloud Computing and Cloud Related IT Professional Services

518210C Includes commercially available cloud computing services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) and emerging cloud computing services, to include cloud based artificial intelligence/machine learning, IT professional services that are focused on providing the types of services that support the Government's adoption of, migration to, or governance/management of cloud computing. Specific cloud related IT professional labor categories and/or fixed-price professional services solutions that support activities associated with assessing cloud solutions, refactoring workloads for cloud solutions, migrating legacy or other systems to cloud solutions, providing management/governance of cloud solutions, DevOps, developing cloud native applications, or other cloud oriented activities are within scope of this SIN.

NOTE: Subject to Cooperative Purchasing

Cooperative Purchasing: Yes
Set Aside: No
FSC/PSC Code : DB10
Maximum Order : \$500,000

NAICS

Number	Description	Business Size
518210	Data Processing, Hosting, and Related Services	\$40 million

Instructions:

Additional SIN Description: This SIN provides access to cloud (e.g., IaaS, PaaS, SaaS) computing services across public, community, and hybrid deployment models. Cloud computing services shall comply with [National Institute of Standards and Technology \(NIST\) Definition of Cloud Computing Essential Characteristics](#) (NIST SP 800-145). Cloud computing that does not meet all NIST essential characteristics are outside the scope of this SIN and shall be assigned to other SINs, where applicable.

Exception for Software as a Service (SaaS): Proposed offerings do not have to meet the first of the five NIST cloud characteristics in [NIST SP 800-145](#); the first NIST cloud characteristic is: “On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.” It is not a SIN 51810C requirement that the SaaS customer be able to (de)provision SaaS access/licenses unilaterally with no human interaction with the SaaS provider.

Cloud related IT professional labor categories are within scope of this SIN. Cloud related IT professional labor categories are not subject to adherence to the NIST definition of cloud computing; therefore, no technical response is required for a labor proposal. Non-professional labor categories subject to Service Contract Labor Standards (SCLS) (e.g., IT help desk support) that are incidental to and used solely to support specific Cloud related IT professional labor categories and/or fixed-price professional services solutions must be offered under a different SIN that specifically covers the proposed services.

Ancillary products and services are not within scope of this SIN. Any items that are not within the scope of this SIN must be offered under a SIN that specifically covers the proposed services.

The following are out of scope for this SIN: cloud “token,” “gift card,” “credit,” or other similar types of prepaid offerings:

- 1.) Cloud computing services (*i.e.*, IaaS, PaaS, SaaS) are sometimes offered commercially as a cloud “token,” “gift card,” “credit,” or require purchase of a prepaid offering; these are out of scope

for this SIN.

2.) Credits for cloud computing services (i.e., IaaS, PaaS, SaaS) that are paid for in advance and spent or used at a later time are commonly termed commercially as a cloud “token,” “gift card,” or “credit”, and are out of scope for SIN 518210C.

Physical hardware, non-cloud software per the NIST definition, and other artifacts acquired to support the physical construction of a private or other cloud are not within the scope of this SIN.

1) Specific Instructions for SIN 518210C – Cloud Computing and Cloud Related IT Professional Services

a) Offerors shall follow instructions and guidance for cloud computing services located on these resource pages: [cloud computer and cloud-related IT professional services](#) and [SIN 518210C Specific Information for Offerors](#).

b) Offerors may propose:

i) Cloud computing services only (i.e., IaaS, PaaS, SaaS) per NIST standards as defined in NIST Special Publication 800-145 “The NIST Definition Cloud Computing”,

ii) Cloud related IT professional services and/or fixed-price cloud professional services solutions that are not subject to NIST standards only; or

c) The offeror must state which cloud computing service model(s), if any, is/are being proposed (i.e., IaaS, PaaS, SaaS).

d) The offeror must state which cloud computing deployment model(s), if any, is/are being proposed (i.e., public, community, and hybrid).

e) Pricing increment of offerings:

i) For all offers of IaaS/PaaS/SaaS and cloud related IT professional services, pricing shall be per a unit of measure.

ii) For all offers of SaaS, regardless of length of license term, pricing to support upfront payment is allowed as long as the software licenses are delivered via SaaS and meet the criteria listed in this Information Technology Category attachment.

f) Acceptance Testing: Acceptance testing shall be performed of the systems for ordering activity approval in accordance with the approved test procedures.

g) Training

i) If training is provided in accordance with standard commercial practices, the offeror shall provide normal commercial installation, operation, maintenance, and engineering interface training on the system.

ii) If there are separate training charges, they should be included in the GSA Price List (I-FSS-600 CONTRACT PRICE LISTS (see current Solicitation for clause effective date)).

h) Information Assurance/Security Requirements: Offerors shall meet information assurance/security requirements in accordance with the ordering activity requirements.

i) Reporting: Offerors shall provide to the ordering activity any general reporting capabilities available to verify performance, cost and availability. In accordance with commercial standard practice, the offeror may furnish the ordering activity with a monthly summary report.

j) Cloud related IT professional services may be listed on SIN 54151S - Information Technology Professional Services. The cloud related IT professional services on this SIN (518210C) shall be cloud specific titles and descriptions. At a minimum, the word “cloud” shall appear both in the title and the description of each labor category or fixed-price professional services solutions proposed for this SIN. The relevant past performance projects must demonstrate that the cloud related IT professional services

were utilized in the IaaS, PaaS, and/or SaaS environment. NOTE: Identical labor categories cannot be on both SINs 54151S and 518210C. It is recommended that cloud-related IT professional services and/or fixed-price professional services solutions that are not subject to NIST standards should be offered under SIN 518210C.

k) Offerors may optionally select a single service model that best fits a proposed cloud computing offering. Only one service model may be selected per each proposed cloud computing offering. Offerors may elect to submit multiple cloud computing offerings, each with its own single service model.

l) Deployment model selection within this SIN is optional for any individual cloud computing offering. Offerings may be included without a deployment model selection so long as they comply with all the essential characteristics of cloud computing as outlined by NIST SP 800-145. The three NIST deployment models within the scope of this SIN are: Public, Community, and Hybrid.

m) All current pricing requirements in provision SCP-FSS-001 apply. At the current time, there is no provision for reducing or eliminating standard price list posting requirements to accommodate rapid cloud price fluctuations.

n) All pricing models for cloud computing services must have the core capability to meet the NIST Essential Cloud Characteristics, particularly with respect to on-demand self-service, while allowing alternate variations at the task order level at agency discretion, pursuant to the guidance on NIST Essential Characteristics.

o) Evaluation factors for cloud related IT professional services, specific cloud labor categories and/or fixed-price professional services solutions are found within this same document under Section II Instructions for all IT Offerors under 6) Relevant Project Experience Evaluation.

2) Specific Evaluation Factor for Cloud Computing Services Adherence to the NIST Essential Cloud Characteristics per NIST SP 800-145.

Within a two-page limitation for each cloud computing service (e.g., IaaS, PaaS, SaaS) submitted, provide a description of how the cloud computing service meets each of the five essential cloud computing characteristics as defined in National Institute of Standards and Technology (NIST) Special Publication 800-145 and subsequent versions of this publication. This standard specifies the definition of cloud computing for use by Federal agencies. Each cloud computing service must be capable of satisfying each of the five NIST essential characteristics as follows:

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service cloud (Pay per use, or pay as you go)

Refer to 518210C. Specific Information for Offerors available on the [Multiple Award Schedule](#) page for guidance on meeting the NIST essential characteristics. For the purposes of the cloud computing and cloud related IT professional services SIN, meeting the NIST essential characteristics is concerned primarily with whether the underlying capability of the commercial service is available, and whether or not an ordering activity actually requests or implements the capability.

3) Cloud Consumption Offerors must identify in their GSA price List (I-FSS-600 CONTRACT PRICE LISTS) all cloud computing services that are available to be ordered on a consumption basis.

SIN Level Regulations:

Regulation Number	Regulation Title/Comments
552.238-81	PRICE REDUCTIONS (DEC 2021) (DEVIATION)

	<p>Instructions: This GSAR clause is prescribed and contained within Acquisition Letter MV-21-06, Supplement 1.</p>
552.238-199	<p>SPECIAL ORDERING PROCEDURES APPLICABLE WHEN PROCURING CLOUD COMPUTING ON A CONSUMPTION BASIS (MAR 2022)</p> <p>Instructions: This GSAR clause is prescribed and contained within Acquisition Letter MV-21-06, Supplement 1.</p>

F02. Electronic Commerce Subcategory

Instructions:
Continuous Diagnostics and Mitigation (CDM) Approved Products

GSA has partnered with the Cybersecurity and Infrastructure Security Agency (CISA) to showcase CISA approved CDM tools. The CISA CDM Program’s Approved Products List (APL) is the authoritative catalog for all approved CDM Tools and associated services. CDM APL Tools will carry the [CDM](#) tools symbol. The full complement of CDM subcategories includes tools, associated maintenance, and other related activities such as training. The CDM products and associated services undergo a DHS CISA product qualification process in order to be added to the CDM Approved Products List (APL). The APL features high-quality cybersecurity vendors offering products and related services to Federal, State, and Local Governments. CISA only accepts submissions to modify the CDM APL monthly. Offerors can submit updates to the APL on the first Monday of the first full or partial week of the month, with submissions being accepted through Friday of that week. A full submission calendar can be found on the CISA [website](#). For technical and CDM APL related questions, please contact the CISA CDM Program Office at (csd_cb.acqbudg@cisa.dhs.gov).

SIN 54151ECOM Electronic Commerce and Subscription Services

54151ECOM Includes value added network services, e-mail services, Internet access services, electronic subscription services, data transmission services, and emerging electronic commerce technologies.

NOTE: Subject to Cooperative Purchasing

Cooperative Purchasing: Yes
Set Aside: No
FSC/PSC Code : DG10
Maximum Order : \$500,000

NAICS

Number	Description	Business Size
541519	Other Computer Related Services	\$34 million

Instructions:

1. Specific Instructions for SIN 54151ECOM - Electronic Commerce and Subscription Services

- a. Acceptance Testing: Acceptance testing shall be performed of the systems for ordering activity approval in accordance with the approved test procedures. Management and operations pricing shall be provided on a uniform basis. All management and operations requirements for which pricing elements are not specified shall be provided as part of the basic service.
- b. Normal commercial installation, operation, maintenance, and engineering interface training on the system shall be provided. If there is a separate charge, it must be stated as an attachment to the GSA Price List (I-FSS-600 CONTRACT PRICE LISTS (see current Solicitation for clause effective date)).

- c. Monthly summary report may be provided to the Ordering Activity in accordance with commercial practice.
2. If an electronic commerce service plan is offered the following must be stated as an attachment to the GSA Price List (I-FSS-600 CONTRACT PRICE LISTS (see current Solicitation for clause effective date)).
 - a. Describe the electronic service plan and eligibility requirements;
 - b. Describe charges, if any, for additional usage guidelines; and
 - c. Describe corporate volume discounts and eligibility requirements, if any.

F03. Financial Management Services Subcategory

Instructions:

Offerors submitting an offer for a SIN(s) under the “Financial Management Services Subcategory” must also comply with the following:

1. The following applies to the Financial Management Quality Service Management Office (FM QSMO) Core Financial Management (FM) Solutions and IT Professional Services SIN that includes Cloud Related IT Professional Services.

- a. Only IT Professional Services or Labor Categories shall be offered
- b. Offerors shall provide résumés to the GSA contracting officer or the user ordering activity upon request.
- c. Offerors shall provide a description of each type of IT Professional Service or Labor Category offered, and it should be presented in the same manner as the Contractor sells to its commercial customers. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles (labor categories) for those individuals who will perform the service must be provided.

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

EXAMPLE: Commercial Job Title: System Engineer

Minimum/General Experience: Three (3) years of technical experience which applies to cloud systems analysis and design techniques for complex computer systems. Requires competence in all phases of systems analysis techniques, concepts, and methods; also requires knowledge of available hardware, system software, input/output devices, structure, and management practices.

Functional Responsibility: Guides users in formulating requirements, advises alternative approaches, and conducts feasibility studies.

- d. Pricing for each type of IT Professional Service or Labor Category shall be in accordance with customary commercial practices; e.g., hourly rates, monthly rates, term rates, and/or fixed prices, minimum general experience, and minimum education.
 - e. Pricing of services shall be offered at the Contractor’s facility and/or at the ordering activity location in accordance with customary commercial practices.
 - f. All awarded professional services/labor categories shall be included as an attachment to the GSA Price List (I-FSS-600 CONTRACT PRICE LISTS (see current Solicitation for clause effective date)) in the format provided above.

2. **Continuous Diagnostics and Mitigation (CDM) Approved Products** - GSA has partnered with the Cybersecurity and Infrastructure Security Agency (CISA) to showcase CISA approved CDM tools. The CISA CDM Program’s Approved Products List (APL) is the authoritative catalog for all approved CDM Tools and associated services. CDM APL Tools will carry the [CDM](#) tools symbol. The full complement of CDM subcategories includes tools, associated maintenance, and other related activities such as training. The CDM products and associated services undergo a DHS CISA product qualification process in order to be

added to the CDM Approved Products List (APL). The APL features high-quality cybersecurity vendors offering products and related services to Federal, State, and Local Governments. CISA only accepts submissions to modify the CDM APL monthly. Offerors can submit updates to the APL on the first Monday of the first full or partial week of the month, with submissions being accepted through Friday of that week. A full submission calendar can be found on the CISA [website](#). For technical and CDM APL related questions, please contact the CISA CDM Program Office at (csd_cb.acqbudg@cisa.dhs.gov).

SIN 518210FM Financial Management Quality Service Management Office (FM QSMO) Core Financial Management (FM) Solutions and IT Professional Services

518210FM Includes Core Financial Management Solutions (Core FS) and Financial Management (FM) services and solutions that are complementary to or augment Core FS and/or support agency modernizations. Offerings include financial management software suites in a cloud environment; services, applications, and modules that help agencies adopt FM QSMO solutions; and IT professional services and/or labor categories, software, cloud computing and IT training that support FM QSMO adoption.

Cooperative Purchasing: Yes
Set Aside: No
FSC/PSC Code : DB10
Maximum Order : \$500,000

NAICS

Number	Description	Business Size
518210	Data Processing, Hosting, and Related Services	\$40 million

Instructions:

For additional SIN subgroup requirements, please visit Financial Management Capabilities Framework (FMCF) website at the following link:

<https://www.fiscal.treasury.gov/fmqsmo/financial-management-capability-framework.html>

SIN 518210FM Subgroups:

1. Core Financial Management Solutions (Core FS) – partially pre-configured commercial financial management software suites offered in a cloud environment. Core FS offerings that are determined acceptable to meet or exceed Core FS functionality scope and Financial Management Capability Framework (FMCF) standards and that can accommodate agency-specific business needs. Items within scope of this subgroup: cloud computing services.
2. Additional Financial Management (FM) Solutions - business capabilities that augment those provided by the Core FS Baseline Solution and have a correlation to Federal Financial Management (FFM) functions or activities. Includes cost management solutions, reporting tools, business information exchange (BIE) solutions, FM business analytics and intelligence. Items within scope of this subgroup: products and professional services/labor categories.
3. Financial Management (FM) Service/Solution Adoption and Transition Services – services to help agencies in identifying, selecting, acquiring, migrating to, and using FM QSMO Marketplace offerings effectively and efficiently. These services may also be needed when extensive or complex FM solution/service changes are released, or significant functionality is removed. Includes strategy and planning, FM data conversion and migration, IV&V, readiness assessments, integration support, project management, and FM solution/service testing. Items within scope of this subgroup: products and professional services/labor categories.
4. Financial Management (FM) Technology Operations Support Services – support and assist with technology implementation and operations. Includes FM technology development, testing, implementation, operations, and maintenance support, information exchanges between FM solutions and services and agency mission systems, service desk, related ancillary training, and support for legacy core financial systems. Items within scope of this subgroup: products, training and professional services/labor categories.

The following are out of scope for this SIN: cloud “token,” “gift card,” “credit,” or other similar types of prepaid offerings:

1. Cloud computing services (i.e., IaaS, PaaS, SaaS) are sometimes offered commercially as a cloud “token,” “gift card,” “credit,” or require purchase of a prepaid offering; these are out of scope for

this SIN.

2. Credits for cloud computing services (i.e., IaaS, PaaS, SaaS) that are paid for in advance and spent or used at a later time are commonly termed commercially as a cloud “token,” “gift card,” or “credit”, and are out of scope for SIN 518210FM.

1) Offerings under SIN 518210FM shall be in accordance with the following standards, as applicable based on offering type and components:

- FMCF Standards and Capabilities
- Federal Integrated Business Framework (FIBF) FFM Functions and Activities
- FIBF FFM Business Use Cases o FIBF FFM Business Capabilities - Federal Financial Management System Requirements (FFMSRs)
- FIBF FFM Business Data Elements o Core FS Pre-Built Business Reports
- Core FS Pre-Built Business Information Exchanges (BIEs)
- FM Technology Design and Operation Capabilities
- FM Solution-Service Evaluation Criteria
- FM Provider Service Measures

The most current versions of FMCF Standards are available at

<https://www.fiscal.treasury.gov/fmqsmo/financial-management-capability-framework.html>

2) Additional submission and evaluation requirements for SIN 518210FM:

a) All submissions for SIN 518210FM must include a cover letter that identifies the SIN subgroups that are being proposed, the required technical evaluation form (Technical Narrative Response Template), the required Solution/Service Definition Template available at [Multiple Award Schedule](#), and the required price proposal template. The Core FS Pre-Built BIE Response Template is only required for Core Financial Management Solutions (Core FS) subgroup, which is available at [Multiple Award Schedule](#).

b) All SIN subgroups will be subject to acceptable/unacceptable technical evaluation that will be performed by the FM QSMO Project Management Office (PMO).

c) Core Financial Management Solutions (Core FS) subgroup: submission and evaluation requirements

i) Written/narrative technical evaluation is required for all offerings under SIN 518210FM.

ii) A sandbox/capabilities demonstration is required. The structure of the sandbox/capabilities demonstration will have a not-to-exceed consecutive eight (8) hour time limit. If offerors/contractors can demonstrate all capabilities in a shorter period of time, the sandbox demonstration will conclude then. FM QSMO PMO will coordinate the scheduling for each vendor’s demonstration.

iii) For the required technical evaluation form (Technical Narrative Response Template) and the required Core FS Pre-Built BIE Response Template, please visit the [Multiple Award Schedule](#) page.

iv) A Target completion timeframe for evaluation of Core FS (including sandbox/capabilities demonstration) is 60 business days.

v) Addition of Core FS subgroup to awarded SIN 518210FM will require written/narrative technical evaluation and sandbox demonstration.

vi) Addition of new items to the awarded Core FS subgroup will require written/narrative technical evaluation and sandbox demonstration.

d) Additional Financial Management (FM) Solutions subgroup: submission and evaluation requirements

i) Written/narrative technical evaluation is required for all offerings under SIN 518210FM.

ii) For the required technical evaluation form (Technical Narrative Response Template), please visit the [Multiple Award Schedule](#) page.

iii) Target completion timeframes for evaluation of Additional Financial Management (FM) Solutions is 20 business days for service-only offerings and 40 business days for service offerings that include technology or other technology offerings.

iv) Addition of Additional FM Solutions subgroup to awarded SIN 518210FM will require written/narrative technical evaluation and sandbox demonstration.

v) Addition of new items to the Additional FM Solutions subgroup will require written/narrative technical evaluation and sandbox demonstration.

e) Financial Management (FM) Service/Solution Adoption and Transition Services subgroup: submission and evaluation requirements

i) Written/narrative technical evaluation is required for all offerings under SIN 518210FM.

ii) For the required technical evaluation form (Technical Narrative Response Template), please visit the [Multiple Award Schedule](#) page.

iii) Target completion timeframes for evaluation of FM Service/Solution Adoption and Transition Services is 20 business days for service-only offerings and 40 business days for service offerings that include technology or other technology offerings.

iv) Addition of FM Service/Solution Adoption and Transition Services to awarded SIN 518210FM will require written/narrative technical evaluation and sandbox demonstration.

v) Addition of new items to the FM Service/Solution Adoption and Transition Services subgroup will require written/narrative technical evaluation.

f) Financial Management (FM) Technology Operations Support Services subgroup: submission and evaluation requirements

i) Written/narrative technical evaluation is required for all offerings under SIN 518210FM.

ii) For the required technical evaluation form (Technical Narrative Response Template), please visit the [Multiple Award Schedule](#) page.

iii) Target completion timeframes for evaluation of FM Technology Operations Support Services is 20 business days for service-only offerings and 40 business days for service offerings that include technology or other technology offerings.

iv) Addition of FM Technology Operations Support Services to awarded SIN 518210FM will require written/narrative technical evaluation and sandbox demonstration.

v) Addition of new items to FM Technology Operations Support Services subgroup will require written/narrative technical evaluation.

3) SIN Subgroups: Offerors may request to be placed in any of the SIN Subgroups. Being awarded specific subgroups is dependent on passing the technical evaluation for both offers and modifications. The government will validate which of the following 4 SIN subgroups apply:

1. Core Financial Management Solutions (Core FS)
2. Additional Financial Management (FM) Solutions
3. Financial Management (FM) Service/Solution Adoption and Transition Services
4. Financial Management (FM) Technology Operations Support Services

a) Following award notification for one or more of the 4 SIN subgroups, awarded contractors may select the corresponding subgroups by following the instructions below:

- i) Login to eBuy
- ii) From the top menu, select "Profile"
- iii) Click "Modify Subgroups"

iv) Select the applicable subgroups according to the instructions

All contractor selections will be monitored by the FM QSMO PMO for compliance and action will be taken against your contract if you select subgroups that have not been awarded under your contract.

F04. IT Hardware Subcategory

Instructions:

1. Offerors submitting an offer for a SIN(s) under the "IT Hardware Subcategory" must also comply with the following:

- a. Installation and Technical Services for new equipment
 - i. Offerors shall indicate as an attachment to the GSA Price List (I-FSS-600 CONTRACT PRICE LISTS (see current Solicitation for clause effective date)):
 - A. if the equipment is self-installable; and/or
 - B. if the equipment is not self-installable, include any fees for installation, training or maintenance
 - ii. Offerors should provide commercial practices for installation, deinstallation and/or reinstallation for review and possible inclusion in the contract.

SIN 33411 Purchasing of New Electronic Equipment

33411 Includes desktop, laptop, tablet computers (including rugged), servers, storage equipment, hyperconverged integrated systems, supercomputers, routers, switches and other communications equipment, IT security equipment (hardware based firewalls), audio and video (AV) equipment, public address systems, monitors/displays, sensors and other Internet of Things (IOT) devices, printers and Multi-Function Device (MFD) equipment, broadcast band radio, two-way radio (LMR), microwave radio equipment, satellite communications equipment, radio transmitters/receivers (airborne), radio navigation equipment/antennas, optical/imaging systems, and associated peripherals required for operations (such as controllers, connectors, cables, drivers, adapters, etc., ancillary installation of any equipment purchased.

NOTE: Subject to Cooperative Purchasing

Cooperative Purchasing: Yes
Set Aside: No
FSC/PSC Code : 7B22
Maximum Order : \$500,000

NAICS

Number	Description	Business Size
334111	Electronic Computer Manufacturing	1250 employees
334112	Computer Storage Device Manufacturing	1250 employees
334210	Telephone Apparatus Manufacturing	1250 employees

Instructions:

****Best-in-Class (BIC) Designation****

1. Specific Instructions for SIN Specific Instructions for SIN 33411 - Purchasing of New Electronic Equipment

- a. Offerors of new equipment are required to provide maintenance service and/or repair service and repair parts, in accordance with normal industry practices, for the type of equipment offered, for the Scope of the Contract (i.e., at minimum, the 48 contiguous states and the District of Columbia).

SIN 532420L Leasing of New Electronic Equipment

532420L Leasing of new electronic equipment. Includes the following lease types: Lease to Ownership, and Lease with Option to Own
 NOTE: Subject to Cooperative Purchasing

Cooperative Purchasing: Yes
Set Aside: No
FSC/PSC Code : DE10
Maximum Order : \$500,000

NAICS

Number	Description	Business Size
532420	Office Machinery and Equipment Rental and Leasing	\$40 million

Instructions:

1. Specific Instructions for SIN 532420L - Leasing of new electronic equipment

a. Two (2) sets of leasing terms and conditions are allowable. Either option or both options may be offered.

i. Option 1 does not contain a cancellation clause and all leases automatically expire on September 30th or sooner. Available on the [Multiple Award Schedule](#) page under SIN 532420L

ii. Option 2 contains a cancellation clause, in which the fee must be in accordance with applicable legal principles. Available on the [Multiple Award Schedule](#) page under SIN 532420L

b. The terms and conditions for each option type(s) offered shall be attached to the GSA Price List (I-FSS-600 CONTRACT PRICE LISTS (see current Solicitation for clause effective date)).

SIN Level Regulations:

Regulation Number	Regulation Title/Comments
52.207-5	OPTION TO PURCHASE EQUIPMENT (FEB 1995)

SIN 811212 Maintenance of Equipment, Repair Services and/or Repair/Spare Parts

811212 Maintenance, Repair Service, and Repair Parts/Spare Parts for Government-Owned General Purpose Commercial Information Technology Equipment, Radio/Telephone Equipment. (After Expiration of Guarantee/Warranty Provisions and/or When Required Service Is Not Covered by Guarantee/Warranty Provisions) and for Leased Equipment

NOTE: Subject to Cooperative Purchasing

Cooperative Purchasing: Yes
Set Aside: No
FSC/PSC Code : DB02
Maximum Order : \$500,000

NAICS

Number	Description	Business Size
811210	ELECTRONIC AND PRECISION EQUIPMENT REPAIR AND MAINTENANCE	\$34 million

Instructions:

1. Specific Instructions for SIN 811212 - Maintenance of Equipment, Repair Services and/or Repair/Spare Parts

- a. Hardware maintenance and/or Service Repair is available, and allow for additional information to complete the "fill-in" to the terms and conditions.
 - i. Repair Service Order Terms available on the Multiple Award Schedule page under SIN 811212
 - ii. Maintenance Order Terms available on the Multiple Award Schedule page under SIN 811212
- b. The terms and conditions for each option type(s) offered shall be attached to the GSA Price List (I-FSS-600 CONTRACT PRICE LISTS (see current Solicitation for clause effective date)).
- c. Hardware maintenance and/or service repair shall be authorized by the OEM.
- d. All parts furnished in connection with the repair and/or maintenance of equipment shall be parts authorized by the OEM.

F05. IT Services Subcategory

Instructions:

Offerors submitting an offer for a SIN(s) under the "IT Services Subcategory" must also comply with the following:

- a. Only IT Professional Services or Labor Categories shall be offered.
- b. Resumes shall be provided to the GSA contracting officer or the ordering activity upon request.
- c. Offerors shall provide a description of each type of IT Professional Service or Labor Category offered, and it should be presented in the same manner as the Contractor sells to its commercial and other ordering activity customers. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles (labor categories) for those individuals who will perform the service should be provided.

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

EXAMPLE: Commercial Job Title: System Engineer

Minimum/General Experience: Three (3) years of technical experience which applies to systems analysis and design techniques for complex computer systems. Requires competence in all phases of systems analysis techniques, concepts and methods; also requires knowledge of available hardware, system software, input/output devices, structure and management practices.

Functional Responsibility: Guides users in formulating requirements, advises alternative approaches, conducts feasibility studies.

- d. Pricing for each type of IT Professional Service or Labor Category shall be in accordance with customary commercial practices; e.g., hourly rates, monthly rates, term rates, and/or fixed prices, minimum general experience and minimum education.
- e. Pricing of services shall be offered at the Contractor's facility and/or at the ordering activity location in accordance with customary commercial practices.
- f. All awarded professional services/labor categories shall be included as an attachment to the GSA Price List (I-FSS-600 CONTRACT PRICE LISTS (see current Solicitation for clause effective date)) in the format provided above.

SIN 54151HACS Highly Adaptive Cybersecurity Services (HACS)

54151HACS Includes a wide range of fields such as, the seven-step Risk Management Framework services, information assurance, virus detection, zero trust architecture, network management, situational awareness and incident response, secure web hosting, backups, security services and Security Operations Center (SOC) services. HACS vendors are cataloged under the 6 subgroups of High Value Asset Assessments; Risk and Vulnerability Assessments, Cyber Hunt, Incident Response, Penetration Testing, and Incident Handling and Event Management (IHEM).

NOTE: Subject to Cooperative Purchasing

Cooperative Purchasing: Yes
Set Aside: No
FSC/PSC Code : DJ01
Maximum Order : \$500,000

NAICS

Number	Description	Business Size
541519	Other Computer Related Services	\$34 million

Instructions:

Additional SIN Description: Includes proactive and reactive cybersecurity services that improve customer enterprise-level security posture. Services to identify and protect a customer's information resources, detect and respond to cybersecurity events or incidents, and recover capabilities or services impaired by any incidents that emerge.

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

The seven-step RMF includes preparation, information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. RMF activities may also include Information Security Continuous Monitoring Assessment (ISCM), which evaluate organization-wide ISCM implementations, and also Federal Incident Response Evaluations (FIREs), which assess an organization's incident management functions.

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

Find the requirements for SIN 54151HACS oral technical evaluation and other guidance for offerors on our [HACS page](#).

1. Specific Instructions for SIN 54151HACS - Highly Adaptive Cybersecurity Services (HACS)

a. Offerors may request to be placed in the following subgroups.

i. High Value Asset (HVA) Assessments include Risk and Vulnerability Assessment (RVA) which assesses threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations. The services offered in the RVA sub-category include Network Mapping, Vulnerability Scanning, Phishing Assessment, Wireless Assessment, Web Application Assessment, Operating System Security Assessment (OSSA), Database Assessment, and Penetration Testing. Security Architecture Review (SAR) evaluates a subset of the agency's HVA security posture to determine whether the agency has properly architected its cybersecurity solutions and ensures that agency leadership fully understands the risks inherent in the implemented cybersecurity solution. The SAR process utilizes in-person interviews, documentation reviews, and leading practice evaluations of the HVA environment and supporting systems. SAR provides a holistic analysis of how a HVA's individual security components integrate and operate, including how data is protected during operations. The SAR uses the RMF when designing and implementing the seven tenets of zero trust architecture by describing how the steps in the RMF map to similar steps described in NIST Special Publication (SP) 800-207, [Zero Trust Architecture](#). Systems Security Engineering (SSE) identifies security vulnerabilities and minimizes or contains risks associated with these vulnerabilities spanning the Systems Development Life Cycle. SSE focuses on, but is not

limited to the following security areas: perimeter security, network security, endpoint security, application security, physical security, and data security.

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

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

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

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

vi. Incident Handling and Event Management (IHEM) ensures that appropriate response activities are conducted when incidents and events are detected. These activities are meant to prevent or reduce impact to enterprise operations and/or security in accordance with multiple industry sources, including National Institute of Standards and Technology (NIST). Functionality includes monitoring organizational assets for deviations from expected activity; detecting and declaring incidents and events; performing analysis, triage, and containment when necessary; and performing remediation and recovery steps.

b. Services offered SIN 54151HACS shall be in accordance with the following laws and standards when applicable to the specific task orders, including but not limited to:

i. Federal Acquisition Regulation (FAR) Part 52.204-21

ii. OMB Memorandum M-17-12 - Preparing for and Responding to a Breach of Personally Identifiable Information (PII)

iii. OMB Memorandum M- 19-03 - Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program

iv. 2017 Report to the President on Federal IT Modernization

v. The Cybersecurity National Action Plan (CNAP)

vi. NIST SP 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems

vii. NIST SP 800-27A - Engineering Principles for Information Technology Security (A Baseline for Achieving Security)

viii. NIST SP 800-30 - Guide for Conducting Risk Assessments

ix. NIST SP 800-35 - Guide to Information Technology Security Services

x. NIST SP 800-37 - Risk Management Framework for Information Systems and Organizations: A Systems Life Cycle Approach for Security and Privacy

xi. NIST SP 800-39 - Managing Information Security Risk: Organization, Mission, and Information System View

xii. NIST SP 800-44 - Guidelines on Securing Public Web Servers

xiii. NIST SP 800-48 - Guide to Securing Legacy IEEE 802.11 Wireless Networks

xiv. NIST SP 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations

- xv. NIST SP 800-61 - Computer Security Incident Handling Guide
- xvi. NIST SP 800-64 - Security Considerations in the System Development Life Cycle
- xvii. NIST SP 800-82 - Guide to Industrial Control Systems (ICS) Security
- xviii. NIST SP 800-86 - Guide to Integrating Forensic Techniques into Incident Response
- xix. NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment
- xx. NIST SP 800-128 - Guide for Security-Focused Configuration Management of Information Systems
- xxi. NIST SP 800-137 - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- xxii. NIST SP 800-153 - Guidelines for Securing Wireless Local Area Networks (WLANs)
- xxiii. NIST SP 800-160 - Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
- xxiv. NIST SP 800-171 - Protecting Controlled Unclassified Information in non-federal Information Systems and Organizations
- xxv. NIST SP 800-207 - Zero Trust Architecture

c. All professional labor categories under SIN 54151S Information Technology Professional Services may remain there, unless the labor categories are specific to SIN 54151HACS.

d. HACS SIN Labor Categories should be in alignment with the [National Initiative for Cybersecurity Careers and Studies \(NICCS\) Workforce Framework for Cybersecurity \(NICE Framework\)](#). The NICE Framework is a nationally focused resource to help employers develop their cybersecurity workforce. It establishes a common lexicon that describes cybersecurity work and workers regardless of where or for whom the work is performed. The NICE Framework applies across public, private, and academic sectors. When writing labor category descriptions, it is recommended to review the NICE Framework so labor category descriptions speak to cybersecurity. To find the most up-to-date NICE Framework Components, visit the [NICE Framework Resource Center website](#).

2. Oral Technical Evaluation for SIN 54151HACS - Highly Adaptive Cybersecurity Services (HACS)

a. Unless otherwise specified, the offeror shall participate in an oral technical evaluation that will be conducted by a Technical Evaluation Board (TEB). The oral technical evaluation will be held at the unclassified level and will be scheduled by the TEB. The oral technical evaluation will be used to assess the offeror's capability to successfully perform the services within the scope of each subgroup as set forth in this solicitation.

An offeror may only be awarded SIN 54151HACS upon successful completion of the Highly Adaptive Cybersecurity Services oral technical evaluation. If the offeror elects to be cataloged under the "Cyber Hunt" and/or "Incident Response" subgroups, additional questions related to those areas will be asked during the HACS Oral Technical Evaluation.

i. ORAL TECHNICAL EVALUATION CONSTRAINTS: The offeror shall identify up to five key personnel, by name and association with the offeror, who will field questions during the oral technical evaluation. The HACS SIN consists of 6 subgroups. The base HACS Oral Technical Evaluation consists of questions related to the 3 subgroups of, High Value Asset Assessments, Risk and Vulnerability Assessments and Penetration Testing. One (1) hour and 40 minutes is allotted for the base HACS Oral Technical Evaluation. The evaluation will be stopped precisely after 1 hour and 40 minutes. Should the offeror elect to be considered for the additional subgroups of Incident Response and Cyber Hunt, an additional 10 minutes will be allotted for each of those subgroups. Should the offeror elect to be considered for the additional subgroup of Incident Handling and Event management (IHEM), 1 additional hour will be allotted for the IHEM subgroup. The TEB Chairperson will be responsible for ensuring the schedule is met and that all offerors are given the same opportunity to present and answer questions.

ii. ORAL TECHNICAL EVALUATION SCHEDULING: The TEB will contact the offeror's authorized negotiator or the signatory of SF 1449 via email to schedule the oral technical

evaluation. Evaluation time slots will be assigned on a first-come-first-served basis. The Government reserves the right to reschedule any offeror's oral technical evaluation at its sole discretion. The oral technical evaluation will be held at facilities designated by the TEB. The exact location, seating capacity, and any other relevant information will be provided when the evaluations are scheduled. The Government may also make accommodations for vendors to participate in the oral evaluations virtually.

iii. PROHIBITION OF ELECTRONIC RECORDING OF THE ORAL TECHNICAL EVALUATION: The offeror may not record or transmit any of the oral evaluation processes. All offeror's electronic devices shall be removed from the room during the evaluation. The offeror is permitted to have a timer in the room during the evaluation, provided by the TEB.

iv. RESUBMISSION RESTRICTIONS FOR UNSUCCESSFUL VENDORS UNDER THIS EVALUATION FACTOR: The TEB will afford the offeror multiple opportunities to achieve the PASS criteria under this evaluation factor through "clarification" questioning, during the Oral Technical Evaluation. Any offeror whom the TEB has found to have NOT PASSED under this evaluation factor shall be FAILED and shall be ineligible to re-submit under the SIN to participate in this evaluation factor for a period of six (6) months following the date of FAILURE.

v. FOR REJECT AND WITHDRAWN OFFERS OR MODIFICATIONS: An offeror or contractor can re-apply for SIN 54151HACS if they are rejected or withdrawn.

1. If an offeror or contractor PASSES the oral technical evaluation but their offer or modification is rejected or withdrawn, they can re-apply within six (6) months after the oral technical evaluation completion date without having to participate in the oral technical evaluation again. When documentation is resubmitted for review for a new offer/modification, include a statement in the cover letter that the capabilities remain current, accurate, and complete as stated during the oral technical evaluation.

2. If an offeror or contractor PASSES the oral technical evaluation but their offer or modification is rejected or withdrawn and they do not re-apply within six (6) months after the oral technical evaluation completion date, they must participate in a new oral technical evaluation in order to add SIN 54151HACS.

b. Oral Technical Evaluation Procedures: The offeror will be evaluated on their knowledge of the proposed services. The oral technical evaluation will require the offeror to respond to a specific scenario and general questions to assess the offeror's expertise. The competencies, criteria and evaluation minimums for the questions are below: All new offerors and modifications must participate in and PASS the base HACS Oral Technical Evaluation. The Oral Technical Evaluation will include, at a minimum, questions on Risk and Vulnerability Assessment (RVA), Security Architecture Review (SAR), Systems Security Engineering (SSE), and Penetration Testing. At the time of submission, all new offerors and modifications can also elect to be cataloged in one or more of the additional subgroups of Cyber Hunt, Incident Response (IR), or Incident Handling and Event Management (IHEM). Should this election be taken, additional questions related to these subgroups will be included in their HACS evaluation and these additional subgroup topics must be PASSED in order to be awarded the elected subgroups.

c. Oral Technical Evaluation Criteria: The offeror's responses to the government's questions during the oral technical evaluation session shall be used to determine whether the offeror has the requisite experience and expertise to perform tasks expected to be performed within the scope of the SIN. The oral technical proposal will be evaluated and rated on a PASS/FAIL basis. The rating definitions provided below will be used for the evaluation of the offeror's responses to questions during the oral evaluation.

d. SIN Subgroups: Upon completion of the oral technical evaluation for both offers and modifications, the government will determine which of the following 6 SIN subgroups apply:

1. High value Asset (HVA) Assessments
2. Risk and Vulnerability Assessment (RVA)
3. Cyber Hunt
4. Incident Response
5. Penetration Testing

6. Incident Handling and Event Management (IHEM)

Following notification that they are eligible for one or more of the 6 SIN subgroups, awarded contractors may select the corresponding subgroups by following the instructions below:

1. Login to eBuy
2. From the top menu, select "Profile"
3. Click "Modify Subgroups"
4. Select the applicable subgroups according to the instructions

All contractor selections will be monitored by GSA for compliance and action will be taken against your contract if you select Subgroups that have not been awarded under your contract.

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

TECHNICAL RATINGS	
Rating	Definition
PASS	The proposal clearly meets the minimum requirements of the solicitation.
FAIL	The proposal does not clearly meet the minimum requirements of the solicitation.

SIN 54151HEAL Health Information Technology Services

54151HEAL Includes a wide range of Health IT services to include connected health, electronic health records, health information exchanges, health analytics, personal health information management, innovative Health IT solutions, health informatics, emerging Health IT research, and other Health IT services.

NOTE: Subject to Cooperative Purchasing

Cooperative Purchasing: Yes
Set Aside: No
FSC/PSC Code : DA01
Maximum Order : \$500,000

NAICS

Number	Description	Business Size
541519	Other Computer Related Services	\$34 million

Instructions:

1. Specific Instructions for SIN 54151HEAL - Health Information Technology Services

a. Services offered SIN 54151HEAL shall be in accordance with the following laws and standards when applicable to the specific task orders, including but not limited to:

- Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- The National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and Special Publications
- Federal Information Security Management Act (FISMA) of 2002

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

SIN 54151S Information Technology Professional Services

54151S IT Professional Services and/or labor categories for database planning and design; systems analysis, integration, and design; programming, conversion and implementation support; network services, data/records management, and testing.

NOTE: Subject to Cooperative Purchasing

Cooperative Purchasing: Yes
Set Aside: No
FSC/PSC Code : DA01
Maximum Order : \$500,000

NAICS

Number	Description	Business Size
541519	Other Computer Related Services	\$34 million

Instructions:

1. Specific Instructions for SIN 54151S – Information Technology Professional Services

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

F06. IT Software Subcategory

Instructions:

****Best-in-Class (BIC) Designation****

Offerors submitting an offer for a SIN(s) under the “IT Software Subcategory” must also comply with the following:

- 1) Technical Support: Without additional charge to the ordering activity, shall provide a hot line technical support number for the purpose of providing user assistance and guidance in the implementation of the software. The technical support number is available shall be available during specified hours.
 - a) At the task or delivery order level, provide a telephone number and hours of operation for technical support hotline; indicate applicable time zone for the hours of operation—i.e., Eastern time, Central, Mountain or Pacific time.
- 2) Descriptions and Equipment Compatibility: Offerors shall include as an attachment to the GSA Price List (I-FSS-600 CONTRACT PRICE LISTS (OCT 2016) a complete description of each software product including the operating systems on which the software can be used. Also included shall be a brief, introductory explanation of the modules and documentation which are offered.
- 3) Right-to-Copy Pricing: Offerors shall insert the discounted pricing for right-to-copy licenses, if commercially available, in an attachment to the GSA Price List (I-FSS-600 CONTRACT PRICE LISTS

(see current Solicitation for clause effective date)).

4) Utilization Limitations

- a) Software acquisition is limited to commercial computer software defined in FAR Part 2.101.
- b) When acquired by the ordering activity, commercial computer software and related documentation shall be subject to the following:
- i.) Title to and ownership of the software and documentation shall remain with the Contractor, unless otherwise specified.
 - ii.) Software licenses are by site and by ordering activity. An ordering activity is defined as a cabinet level or independent ordering activity. The software may be used by any subdivision of the ordering activity (service, bureau, division, command, etc.) that has access to the site the software is placed at, even if the subdivision did not participate in the acquisition of the software. Further, the software may be used on a sharing basis where multiple agencies have joint projects that can be satisfied by the use of the software placed at one ordering activity's site. This would allow other agencies access to one ordering activity's database. For ordering activity public domain databases, user agencies and third parties may use the computer program to enter, retrieve, analyze and present data. The user ordering activity will take appropriate action by instruction, agreement, or otherwise, to protect the Contractor's proprietary property with any third parties that are permitted access to the computer programs and documentation in connection with the user ordering activity's permitted use of the computer programs and documentation. For purposes of this section, all such permitted third parties shall be deemed agents of the user ordering activity.
 - iii.) Except as provided above, the ordering activity shall not provide or otherwise make available the software or documentation, or any portion thereof, in any form, to any third party without the prior written approval of the Contractor. Third parties do not include prime Contractors, subcontractors and agents of the ordering activity who have the ordering activity's permission to use the licensed software and documentation at the facility, and who have agreed to use the licensed software and documentation only in accordance with these restrictions. This provision does not limit the right of the ordering activity to use software, documentation, or information therein, which the ordering activity may already have or obtains without restrictions.
 - iv.) The ordering activity shall have the right to use the software and documentation with the run-time computing environment (e.g. operating system, virtual machine, mobile operating system, processor etc.) to be specifically identified for which it is acquired at any other facility/user device to which that time computing environment may be transferred, or in cases of Disaster Recovery, the ordering activity has the right to transfer the software to another site/user device if the ordering activity site for which it is acquired is deemed to be unsafe for ordering activity personnel; to use the software and documentation with a backup time computing environment when the primary is inoperative; to copy computer programs for safekeeping (archives) or backup purposes; to transfer a copy of the software to another site/user for purposes of benchmarking new hardware and/or software; and to modify the software and documentation or combine it with other software, provided that the unmodified portions shall remain subject to these restrictions.
 - v.) "Commercial Computer Software" may be marked with the Contractor's standard commercial restricted rights legend, but the schedule contract and schedule pricelist, including this clause, "Utilization Limitations" are the only governing terms and conditions, and shall take precedence and supersede any different or additional terms and conditions included in the standard commercial legend.
 - vi.) Licensee Data belongs exclusively to Licensee, regardless of where the Data may reside at any moment in time including, but not limited to Licensor hardware, networks or other infrastructure and facilities where Data may reside, transit through or be stored from time to time. Licensor makes no claim to a right of ownership in Licensee Data. Licensor agrees to keep the Licensee Data Confidential as that term is defined in the relevant FAR and DFARS provisions pertaining to Confidential Information and Confidentiality. Licensor is not permitted to use Licensee's data for a purpose that is not explicitly granted in writing by Licensee. Upon Licensee request, for any reason whatsoever, Licensor must promptly return all Licensee Data in Licensor's possession in a format as may be designated at the time of request by Licensee.
 - vii.) Licensee may create or hire others (including Licensor) to create modifications,

customizations or other enhancements to the Software which might be classified as "Derivative Works" of the software. Unless otherwise negotiated and mutually agreed upon at the order level, the intellectual property (IP) rights to the Derivative Works shall be owned by the owner of the underlying intellectual property. The Derivative Work[s] shall be made available to the Licensee through a royalty free, perpetual worldwide, no charge license to the Licensee.

5) Continuous Diagnostics and Mitigation (CDM) Approved Products

GSA has partnered with the Cybersecurity and Infrastructure Security Agency (CISA) to showcase CISA approved CDM tools. The CISA CDM Program's Approved Products List (APL) is the authoritative catalog for all approved CDM Tools and associated services. CDM APL Tools will carry the CDM tools symbol. The full complement of CDM subcategories includes tools, associated maintenance, and other related activities such as training. The CDM products and associated services undergo a DHS CISA product qualification process in order to be added to the CDM Approved Products List (APL). The APL features high-quality cybersecurity vendors offering products and related services to Federal, State, and Local Governments. CISA only accepts submissions to modify the CDM APL monthly. Offerors can submit updates to the APL on the first Monday of the first full or partial week of the month, with submissions being accepted through Friday of that week. A full submission calendar can be found on the CISA [website](#). For technical and CDM APL related questions, please contact the CISA CDM Program Office at (csd_ch.acqbudg@cisa.dhs.gov).

SIN 511210 Software Licenses

511210 Includes both term and perpetual software licenses and maintenance. Includes operating system software, application software, EDI translation and mapping software, enabled email message based applications, Internet software, database management applications, and other software.

NOTE: Subject to Cooperative Purchasing

Cooperative Purchasing: Yes
Set Aside: No
FSC/PSC Code : 7A21
Maximum Order : \$500,000

NAICS

Number	Description	Business Size
513210	SOFTWARE PUBLISHERS	\$47 million

Instructions:

Additional SIN Description: Term Licenses. The word "Term" is defined in this Solicitation as "a limited period of time". Term Software Licenses have a limited duration and are not owned in perpetuity. Unless Offerors provide an option for converting Term licenses into perpetual licenses, users lose the right to use these licenses upon the end of the term period. This SIN is NOT Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS) as defined in SIN 518210C - Cloud Computing and Cloud Related IT Professional Services. Term Software Licenses are distinct from Electronic Commerce and Subscription Services (SIN 54151ECOM).

Perpetual Licenses. The word "perpetual" is defined in this Solicitation as "continuing forever, everlasting, valid for all time."

Software maintenance as a product includes the publishing of bug/defect fixes via patches and updates/upgrades in function and technology to maintain the operability and usability of the software product. It may also include other no charge support that is included in the purchase price of the product in the commercial marketplace. No charge support includes items such as user blogs, discussion forums, online help libraries and FAQs (Frequently Asked Questions), hosted chat rooms, and limited telephone, email and/or web-based general technical support for users self-diagnostics.

Software Maintenance as a product is billed at the time of purchase.

Software maintenance as a product does NOT include the creation, design, implementation, integration, etc. of a software package. These examples are considered software maintenance services under SIN 54151

Software Maintenance Services.

1.) Specific Instructions for SIN 511210 - Software Licenses

a.) Offerors are encouraged to identify within their software items any component interfaces that support open standard interoperability. An item's interface may be identified as interoperable on the basis of participation in a Government agency-sponsored program or in an independent organization program.

b.) The words "term software" or "perpetual software" shall be the first word in the product title/name for: 1) the price proposal template and 2) the SIP file for GSA Advantage. The word "term software" or "perpetual software" shall be the first word in the product title/name for the GSA Pricelist pricing charts (I-FSS-600 CONTRACT PRICE LISTS (see current Solicitation for clause effective date)). The words "term software" or "perpetual software" shall be in each product title in any response to a customer Request for Quote (RFQ) or Request for Information (RFI).

c.) Contractors are encouraged to offer SIN 54151 Software Maintenance Services in conjunction with SIN 511210 - Software Licenses.

d.) Conversion From Term License To Perpetual License

i.) When standard commercial practice offers conversions of term licenses to perpetual licenses, and an ordering activity requests such a conversion, the contractor shall provide the total amount of conversion credits available for the subject software within ten (10) calendar days after placing the order.

ii.) When conversion credits are provided, they shall continue to accrue from one contract period to the next, provided the software has been continually licensed without interruption.

iii.) The term license for each software product shall be discontinued on the day immediately preceding the effective date of conversion from a term license to a perpetual license.

iv.) When conversion from term licenses to perpetual licenses is offered, the price the ordering activity shall pay will be the perpetual license price that prevailed at the time such software was initially ordered under a term license, or the perpetual license price prevailing at the time of conversion from a term license to a perpetual license, whichever is the less, minus an amount equal to a percentage of all term license payments during the period that the software was under a term license within the ordering activity.

e.) Term License Cessation

i.) After a software product has been on a continuous term license for a period of _____ (Fill-in the period of time.) months, a fully paid-up, non-exclusive, perpetual license for the software product shall automatically accrue to the ordering activity. The period of continuous term license for automatic accrual of a fully paid-up perpetual license does not have to be achieved during a particular fiscal year; it is a written Contractor commitment which continues to be available for software that is initially ordered under this contract, until a fully paid-up perpetual license accrues to the ordering activity. However, should the term license of the software be discontinued before the specified period of the continuous term license has been satisfied, the perpetual license accrual shall be forfeited. Contractors who do not commercially offer conversions of term licenses to perpetual licenses shall indicate that their term licenses are not eligible for conversion at any time.

ii.) Each separately priced software product shall be individually enumerated, if different accrual periods apply for the purpose of perpetual license attainment.

iii.) Fill-in data and specific terms shall be attached to the GSA Price List (I-FSS-600 CONTRACT PRICE LISTS (see current Solicitation for clause effective date)).

iv.) The Contractor agrees to provide updates and software maintenance services for the software after a perpetual license has accrued, at the prices and

terms of SIN 54151 - Software Maintenance Services, if the licensee elects to order such services. Title to the software shall remain with the Contractor.

f.) Utilization Limitations for Perpetual Licenses

i.) Software Asset Identification Tags (SWID) (Option 1 Perpetual License)

1.) Option 1 is applicable when the Offeror agrees to include the International Organization for Standardization/International Electrotechnical Commission 19770-2 (ISO/IEC 19770- 2:2015) standard identification tag (SWID Tag) as an embedded element in the software. An ISO/IEC 19970-2 tag is a discoverable identification element in software that provides licensees enhanced asset visibility. Enhance visibility supports both the goals of better software asset management and license compliance. Offerors may use the National Institute of Standards and Technology (NIST) document "NISTIR 8060: Guidelines for Creation of Interoperable Software Identification (SWID) Tags," December 2015 to determine if they are in compliance with the ISO/IEC 19770-2 standard.

2.) Section 837 of The Federal Information Technology Acquisition Reform Act (FITARA) of 2014, requires GSA to seek agreements with software vendors that enhance government- wide acquisition, shared use, and dissemination of software, as well as compliance with end user license agreements. The Megabyte Act of 2016 requires agencies to inventory software assets and to make informed decisions prior to new software acquisitions. In June of 2016, the Office of Management and Budget issued guidance on software asset management requiring each CFO Act (Public Law 101-576 – 11/15/1990) agency to begin software inventory management (M-16-12). To support these requirements, Offerors may elect to include the terms of Option 1 and/or Option 2, which support software asset management and government-wide reallocation or transferability of perpetually licensed software.

ii.) Reallocation of Perpetual Software (Option 2 Perpetual License)

1.) The purpose of SIN 511210 OPTION 2 is to allow ordering activities to transfer software assets for a pre-negotiated charge to other ordering activities.

2.) When an ordering activity becomes aware that a reusable software asset may be available for transfer, it shall contact the Contractor, identify the software license or licenses in question, and request that these licenses be reallocated or otherwise made available to the new ordering activity.

3.) Contractors shall release the original ordering activity from all future obligations under the original license agreement and shall present the new ordering activity with an equivalent license agreement. When the new ordering activity agrees to the license terms, henceforth any subsequent infringement or breach of licensing obligations by the new ordering activity shall be a matter exclusively between the new ordering activity and the Contractor.

4.) The original ordering activity shall de-install, and/or make unusable all of the software assets that are to be transferred. It shall have no continuing right to use the software and any usage shall be considered a breach of the Contractor's intellectual property and a matter of dispute between the original ordering activity/original license grantee and the licensor.

5.) As a matter of convenience, once the original licenses are deactivated, di-installed, or made otherwise unusable by the original ordering activity or license grantee, the Contractor may elect to issue new licenses to the new ordering activity to replace the old licenses. When new licenses are not issued, the Contractor shall provide technical advice on how best to achieve the functional transfer of the

software assets.

6.) Software assets that are eligible for transfer that have lapsed Software Maintenance Services (SIN 54151) may require a maintenance reinstatement fee, chargeable to the new ordering activity or license grantee. When such a fee is paid, the new ordering activity shall receive all the rights and benefits of Software Maintenance Services.

7.) When software assets are eligible for transfer, and are fully covered under pre-paid Software Maintenance Services (SIN 54151), the new ordering activity shall not be required to pay maintenance for those license assets prior to the natural termination of the paid for maintenance period. The rights associated with paid for current Software Maintenance Services shall automatically transfer with the software licenses without fee. When the maintenance period expires, the new ordering activity or license grantee shall have the option to renew maintenance.

8.) The administrative fee to support the transfer of licenses, exclusive of any new incremental licensing or maintenance costs shall be _____ percentage (%) of the original license fee. The fee shall be paid only at the time of transfer. In applying the transfer fee, the Software Contractor shall provide transactional data that supports the original costs of the licenses.

9.) Fill-in data and specific terms shall be attached to the GSA Price List (I-FSS-600 CONTRACT PRICE LISTS (see current Solicitation for clause effective date)).

g.) Software Conversions: Full monetary credit will be allowed to the ordering activity when conversion from one version of the software to another is made as a result of a change in operating system, or from one computer system to another. Under a perpetual license, the purchase price of the new software shall be reduced by the amount that was paid to purchase the earlier version. Under a term license, if conversion credits had accrued while the earlier version was under a term license, those credits shall carry forward and remain available as conversion credits which may be applied towards the perpetual license price of the new version.

SIN 54151 Software Maintenance Services

54151 Software maintenance services creates, designs, implements, and/or integrates customized changes to software that solve one or more problems and is not included with the price of the software. Software maintenance services includes person-to-person communications regardless of the medium used to communicate: telephone support, online technical support, customized support, and/or technical expertise which are charged commercially.

NOTE: Subject to Cooperative Purchasing

Cooperative Purchasing: Yes
Set Aside: No
FSC/PSC Code : DA01
Maximum Order : \$500,000

NAICS

Number	Description	Business Size
541511	Custom Computer Programming Services	\$34 million
541512	Computer Systems Design Services	\$34 million

Instructions:

Additional SIN Description: Software maintenance services are billed in arrears in accordance with 31 U.S.C. 3324.

1. Specific Instructions for SIN 54151 – Software Maintenance Services

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

F07. IT Solutions Subcategory

Instructions:

Offerors submitting an offer for a SIN(s) under the “IT Solutions Subcategory” must also comply with the following:

- a. Only IT Professional Services or Labor Categories shall be offered.
- b. Resumes shall be provided to the GSA contracting officer or the ordering activity upon request.
- c. Offerors shall provide a description of each type of IT Professional Service or Labor Category offered, and it should be presented in the same manner as the Contractor sells to its commercial and other ordering activity customers. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles (labor categories) for those individuals who will perform the service should be provided.

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

EXAMPLE: Commercial Job Title: System Engineer

Minimum/General Experience: Three (3) years of technical experience which applies to cloud systems analysis and design techniques for complex computer systems. Requires competence in all phases of systems analysis techniques, concepts, and methods; also requires knowledge of available hardware, system software, input/output devices, structure, and management practices.

Functional Responsibility: Guides users in formulating requirements, advises alternative approaches, and conducts feasibility studies.

- d. Pricing for each type of IT Professional Service or Labor Category shall be in accordance with customary commercial practices; e.g., hourly rates, monthly rates, term rates, and/or fixed prices, minimum general experience and minimum education.
- e. Pricing of services shall be offered at the Contractor's facility and/or at the ordering activity location in accordance with customary commercial practices.
- f. All awarded professional services/labor categories shall be included as an attachment to the GSA Price List (I-FSS-600 CONTRACT PRICE LISTS (see current Solicitation for clause effective date)) in the format provided above.

Continuous Diagnostics and Mitigation (CDM) Approved Products

GSA has partnered with the Cybersecurity and Infrastructure Security Agency (CISA) to showcase CISA approved CDM tools. The CISA CDM Program's Approved Products List (APL) is the authoritative catalog for all approved CDM Tools and associated services. CDM APL Tools will carry the [CDM](#) tools symbol. The full complement of CDM subcategories includes tools, associated maintenance, and other related activities such as training. The CDM products and associated services undergo a DHS CISA product qualification process in order to be added to the CDM Approved Products List (APL). The APL features high-quality cybersecurity vendors offering products and related services to Federal, State, and Local Governments. CISA only accepts submissions to modify the CDM APL monthly. Offerors can submit updates to the APL on the first Monday of the first full or partial week of the month, with submissions being accepted through Friday of that week. A full submission calendar can be found on the CISA [website](#). For technical and CDM APL related questions, please contact the CISA CDM Program Office at (csd_ch.acqbudg@cisa.dhs.gov).

SIN 541370GEO Earth Observation Solutions

541370GEO Provides geospatial earth observation technologies, products, and services to include, but not limited to ground, satellite and aerial based sensor data and imagery; worldwide digital transmission, internet, data, and video services and products through various networks, platforms, and applications. Offerings include global coverage, imagery, analysis, as a service, change detection, human geography, observation as a service, archive storage and distribution, monitoring, basemaps (mosaics), and earth observation solutions for accurate, mission critical information for uses to include, but not limited to, environmental, agriculture, meteorology, forestry, fish & wildlife habitats, disaster response and recovery, defense, maritime, mapping, humanitarian support, transportation, and public safety.

NOTE: Subject to Cooperative Purchasing

Cooperative Purchasing: Yes
Set Aside: No
FSC/PSC Code : DG11
Maximum Order : \$1,000,000

NAICS

Number	Description	Business Size
541370	Surveying and Mapping (except Geophysical) Services	\$19 million

Instructions:

Additional SIN Description: Includes direct-downlink and delivery services including ground and mobile ground terminals, direct access service, direct to cell phones, ships, and aircraft. Provides solutions based on commercially available dedicated, shared, or on-demand satellite resources and associated terrestrial components and/or airborne constellation/platforms including Unmanned Aerial Systems (UAS). This includes, but not limited to, ground, satellite-based or airborne communications, sensor data, imagery and geospatial collected or derived services and/or products. Sensor data includes electro-optical; synthetic aperture radar; Hyperspectral; LiDAR, geomagnetic field; gravity field, thermal, sonar, and all other current and emerging technologies.

Includes remote sensing and analytic software products, software applications, software data management and analysis, and cloud applications. The full range of end-to-end data services are in the scope of this SIN to include, but not limited to, advanced data analytics, crowdsourcing, change detection, alert notification, machine learning, and emerging technologies and solutions.

IT Professional Services are included in this SIN.

1) Specific Instructions for SIN 541370GEO - Earth Observation Solutions

a) Offerings shall comply with cited Department of Defense (DoD) standards, Intelligence Community (IC) standards, Open Geospatial Consortium (OGC) standards (<http://www.opengeospatial.org/standards>), and other standards such as <https://nationalmap.gov/standards> as specified by the ordering activity.

b) Information Assurance/Security Requirements

i) Offerors shall meet information assurance and security requirements in accordance with the ordering activity requirements.

ii) Offerors shall be capable of meeting at least the minimum-security requirements assigned against a low-impact information system.

c) Technical Support:

i) Without additional charge to the ordering activity, shall provide a hot line technical support number for the purpose of providing user assistance and guidance in the implementation of the software. The technical support number is available shall be available during specified hours.

ii) At the task or delivery order level, provide a telephone number and hours of operation for technical support hotline; indicate applicable time zone for the hours of operation—i.e., Eastern time, Central, Mountain or Pacific time.

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

SIN 541519CSP Credential Service Providers (CSP)

Managed service offering for component or full service Credential Service Providers (CSPs) that meet the requirements of NIST SP 800-63 Digital Identity Guidelines (current version), to include public facing and enterprise.

NOTE: Subject to Cooperative Purchasing.

Cooperative Purchasing: Yes
Set Aside: No
FSC/PSC Code : DJ01
Maximum Order : \$500,000

NAICS

Number	Description	Business Size
541519	Other Computer Related Services	\$34 million

Instructions:

Specific Instructions for SIN 541519CSP – Credential Service Providers (CSP)

- 1) Offeror shall meet all normative requirements of NIST SP 800-63 Digital Identity Guidelines for target assurance levels required or demonstrate comparable alternatives with assurance obtained through certification from the Kantara Initiative, or other GSA approved third party certifier, and be classified as either “Full-Service Credential Service Provider” or “Component Service.”
- 2) Services offered shall be in accordance with the following laws, guidelines, and standards when applicable to specific task orders, including but not limited to:
 - a. Executive Order 14028 Improving the Nation’s Cybersecurity
 - b. OMB Memorandum M-22-09 – Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
 - c. OMB Memorandum M-19-17 – Enabling Mission Delivery through Improved Identity, Credential, and Access Management
 - d. OMB Memorandum M-17-12 – Preparing for and Responding to a Breach of Personally Identifiable Information (PII)
 - e. NIST SP 800-37 – Risk Management Framework for Information Systems and Organizations: A Systems Life Cycle Approach for Security and Privacy
 - f. NIST SP 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations
 - g. NIST SP 800-171 – Protecting Controlled Unclassified Information (CUI)
 - h. DHS CISA Zero Trust Maturity Model
 - i. Voluntary Product Accessibility Template (VPAT)
 - j. World Wide Web Consortium (W3C)
- 3) Notwithstanding any terms or conditions of a Commercial Supplier Agreement (CSA) governing the products or services offered under this SIN, the United States Government, as represented by GSA and including any Department, agency, or other instrumentality of the United States government, as well as any official, employee, or agent of such Department, agency or instrumentality (collectively, “U.S. Government”), reserves the right to assert that the laws of any foreign jurisdiction (including without limitation the General Data Protection Regulations (GDPR) of the European Union) or any U.S. state (including without limitation the California Consumer Privacy Act (CCPA)) pertaining to data protection or data privacy do not apply to the U.S. Government. No terms or conditions stated in the CSA, or any documents attached or referenced therein impose any obligation on the U.S. Government under such laws. Further, the execution of the CSA does not imply any waiver by the U.S. Government of sovereign immunity or of any other privilege or immunity under international law or under the laws of any foreign jurisdiction or any

U.S. state, and the U.S. Government hereby expressly reserves its right and authority to assert all such privileges and immunities.

4) Pricing for all CSP services shall be in accordance with standard commercial practices; and Federal statutes, policy, and regulations e.g., transaction, successful proofs, subscription, and/or fixed prices.

- a. Offeror shall propose volume discounts as part of the pricing model.
- b. Offeror shall propose discounts for re-use and/or re-proof, if applicable to service offering.

5) Offeror has the ability to identify proof members of the public, including: a. US citizens and non-citizens (e.g. green card holders, visa holders). b. Those living in the United States or abroad.

6) Offeror shall provide multi-language support.

7) Offeror shall report key performance metrics which could include:

- a. Pass rates,
- b. Fail rate,
- c. Abandonment,
- d. Fraud rates,
- e. Time to verify.

8) Offerors shall have the ability to detect, prevent, investigate, and provide user account recovery and recourse for fraud and victims of identity theft. Offerors SHOULD include phishing-resistant authentication, social engineering prevention, and the ability to identify and proactively stop fraud both during and after verification (i.e., notices to agencies of fraud attach vectors).

- a. Offeror must submit detailed fraud incident response and recovery plans that can be tailored to meet customer specific scenarios, which include provisions for communication, user notification and support, response activities, recovery of services, and working with external entities like law enforcement.

9) Offeror shall offer multiple verification pathways conformant to NIST SP 800-63 assurance levels.

10) Upon awarding of SIN 541519CSP, customers reserve the right to request additional requirements, based on risk profile/assessments, etc. (e.g., Trust Framework or Inter-System Agreement). a. Offeror may be required to comply with Proof of Concept and/or integration testing.

11) Should GSA update the SIN's technical requirements, MAS contract holders have six (6) months following publication/refresh to comply with new requirements or GSA reserves the right to offboard.

The following are out of scope for this SIN: cloud "token," "gift card," "credit," or other similar types of prepaid offerings:

- 1) Cloud computing services (i.e., IaaS, PaaS, SaaS) are sometimes offered commercially as a cloud "token," "gift card," "credit," or require purchase of a prepaid offering; these are out of scope for this SIN.
- 2) Credits for cloud computing services (i.e., IaaS, PaaS, SaaS) that are paid for in advance and spent or used at a later time are commonly termed commercially as a cloud "token," "gift card," or "credit", and are out of scope for SIN 541519CSP.

Technical Evaluation Criteria

- 1) Offeror must either be listed on the Kantara Trust List or provide a letter from the Kantara Initiative, or other GSA approved third party validating NIST SP 800-63 assurance levels.
- 2) For cloud-based providers, offeror shall hold a FedRAMP Moderate Authorization to Operate (ATO) or be "in process: (offeror must be listed on FedRAMP.gov)
- 3) Offeror applying for inclusion on this SIN will be required to complete a Credential Service Provider (CSP) Capabilities Template located on idmanagement.gov.

4) Additional requirements that shall be addressed in the Relevant Project experience narrative for SIN 541519CSP – Credential Service provider:

- a. Each completed example of project experience shall have been completed within the last two years. All examples of completed services shall have been NIST SP 800-63 compliant identity proofing, credential management, and/or authentication projects.
- b. Provide customer/agency name, dates, detailed description and background information on the project or projects presented to demonstrate CSP expertise.
- c. Outline how the project or projects are related to SIN 541519CSP.

SIN 541519ICAM Identity, Credentialing and Access Management (ICAM)

541519ICAM Managed service offerings for electronic credentials (assurance levels IAL, AAL, and FAL), identity and access management, authentication, and identity and access management professional services.

NOTE: Subject to Cooperative Purchasing

Cooperative Purchasing: Yes
Set Aside: No
FSC/PSC Code : DJ01
Maximum Order : \$1,000,000

NAICS

Number	Description	Business Size
541519	Other Computer Related Services	\$34 million

Instructions:

Additional SIN Description: IT Professional Services are included in this SIN.

1) Specific Instructions for SIN 541519ICAM - Identity, Credentialing and Access Management (ICAM)

a) Description Of Authentication Products, Services And Pricing

- i) Offerors shall provide a description of each type of Authentication Product and Service offered.
- ii) Authentication Products and Services shall be offered in accordance with standard commercial practice.
- iii) Pricing for all Authentication Products and Services shall be in accordance with standard commercial practices; e.g., hourly rates, monthly rates, term rates, and/or fixed prices.

SIN 541519PIV Homeland Security Presidential Directive 12 Product and Service Components

541519PIV PIV products and PIV services to implement the requirements of HSPD-12, FIPS-201 and associated NIST special publications. Implementation components specified under this SIN are: * PIV enrollment and registration services, * PIV systems infrastructure, * PIV card management and production services, * PIV card finalization services, * Logical access control products and services, * PIV system integration services. Installation services and FIPS 201 compliant PACS (Physical Access Control System) products.

NOTE: Subject to Cooperative Purchasing

Cooperative Purchasing: Yes
Set Aside: No

FSC/PSC Code : DJ01
Maximum Order : \$1,000,000

NAICS

Number	Description	Business Size
541519	Other Computer Related Services	\$34 million

Instructions:

Additional SIN Description: Implementation components specified under this SIN are:

- PIV enrollment and registration services,
- PIV systems infrastructure,
- PIV card management and production services,
- PIV card finalization services,
- Logical access control products and services,
- PIV system integration services. Installation services, and
- FIPS 201 compliant PACS (Physical Access Control System) products.

The Approved Products List can be accessed at idmanagement.gov. Use the search bar to find the Approved Products List.

HSPD-12 Product and Service components facilitate trusted physical and electronic access to government facilities and networks using smart card technology. Personal Identity Verification (PIV) Credentials and Services are a key enabler of identity assurance for access control and protect Federal facilities and information systems from unauthorized access, interception, and tampering.

i) Specific Instructions for SIN 541519PIV - Homeland Security Presidential Directive 12 Product and Service Components

a) Description Of Authentication Products, Services And Pricing

i) Offerors shall provide a description of each type of Authentication Product and Service offered.

ii) Authentication Products and Services shall be offered in accordance with standard commercial practice.

iii) Pricing for all Authentication Products and Services shall be in accordance with standard commercial practices; e.g., hourly rates, monthly rates, term rates, and/or fixed prices.

iv) HSPD-12 Product and Service Components:

A) Bundled equipment pricing is requested for the following product components:

- enrollment and registration products,
- PIV card management and production products,
- PIV card activation and
- finalization products.

B) Seat pricing is requested for the following service components offered as managed services:

- enrollment and registration products,
- PIV card management and production products,
- PIV card activation and

- finalization products.

C) Bundled equipment categories, managed service categories and the requirements for bundled equipment and managed service Qualification Requirements are presented at the website: <http://www.idmanagement.gov/>

v) Fill-in data and specific terms shall be attached to the GSA Price List (I-FSS-600 CONTRACT PRICE LISTS (see current Solicitation for clause effective date)).

SIN Level Regulations:

Regulation Number	Regulation Title/Comments
552.238-109	AUTHENTICATION SUPPLIES AND SERVICES (MAY 2019)

SIN 541519PKI Public Key Infrastructure (PKI) Shared Service Providers (PKI SSP) Program

541519PKI PKI SSPs shall provide reliable, authenticated, policy-compliant service offerings to support Federally issued Personal Identity Verification (PIV), Personal Identity Verification Interoperable (PIV-I), and associated certificates and cryptographic key service offerings. In accordance with 40 U.S.C. Federal and State agencies and Tribal organizations can leverage these service offerings to allow authorized personnel physical access to facilities and logical access to networks in accordance with X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework

NOTE: Subject to Cooperative Purchasing

Cooperative Purchasing: Yes
Set Aside: No
FSC/PSC Code : DJ10
Maximum Order : \$1,000,000

NAICS

Number	Description	Business Size
541519	Other Computer Related Services	\$34 million

Instructions:

Additional SIN Description: Policy for the U.S. Federal PKI Common Policy Framework. Digital Certificate Service Providers whose services are deemed to be compliant will be eligible to participate in the PKI SSP program.

The PKI SSP Program enables secure communication and access for government organizations to securely communicate with external partners and comply with key cybersecurity mandates, directives, and policies. PKI SSPs shall provide reliable, authenticated, policy-compliant service offerings to support Federally issued Personal Identity Verification (PIV), Personal Identity Verification Interoperable (PIV-I), and associated certificates and cryptographic key service offerings. Agencies can leverage these service offerings to allow authorized personnel physical access to facilities and logical access to networks. PKI SSPs may only procure X.509 digital certificates and managed PKI services that meet the requirements established in FIPS 201. Offeror shall submit the following:

- A Certification Authority (CA) capable of issuing digital certificates and Certificate
- Revocation Lists (CRLs) compliant with COMMON;
- A publicly accessible repository capable of hosting certificate validation artifacts (e.g., CA certificates and CRLs for retrieval);
- Key management services such as private key escrow and recovery (to include third-party key recovery); and
- Online Certificate Status Protocol (OCSP) validation services.

NOTE: Federal agencies are advised that any authentication products they procure in order to facilitate access to Federal resources by external partners must meet the requirements of the E-Authentication Guidance for

Federal Agencies for the level of assurance identified for the identified Federal resources.

1) Specific Instructions for SIN 541519PKI - Public Key Infrastructure (PKI) Shared Service Providers (PKI SSP) Program

a) Offerors shall comply with the Federal Public Key Infrastructure (FPKI) Policies to include: X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework (FCPF), hereafter referenced as COMMON and its associated change proposals, Key Recovery Policy, U.S. Federal Certificate Profiles: X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program, and the Memorandum of Agreements (MOAs) established between the FPKI Policy Authority (FPKIPA) and the Offeror. In addition, any certificates, associated certificates, and public key pairs issued to the ordering activity will be owned by the government. In addition, the offeror shall be responsible for:

i) Obtaining an Approval to Operate (ATO) declaration through GSA's formal program for information security management before rendering PKI solutions, as well as staying in compliance with FISMA and GSA requirements for protecting GSA IT resources.

ii) Providing written notification to the ordering activity about the intent to change the business relationship in a timely manner so as not to disrupt any PKI services.

iii) Providing a transition plan that includes all activities from transferring a PKI solution to resolution of impacts on end users and the delivery environment. The depth of a transition plan should be appropriate for the type of transition and the criticality of the PKI components going through transition. At a minimum, the activities in the transition plan must be compliant with the COMMON and address the following:

A) The coordination and scheduling of transferring system archives, system inventory and configuration data, certificate profiles, key recovery databases (if applicable), private keys, key shares, audit records, hardware security modules, certificate and certificate revocation list (CRL) databases, and all policy and security documents applicable to the operations of the PKI solution.

B) The estimated costs for terminating, transferring, selling, or disposing a PKI solution must be shared if direct or indirect expenses will be transferred to the new approved PKI solution and/or the impacted customer.

C) The continued services for all certificates and certificate revocation and status checking until the expiration of the longest-lived certificate or transference of the control for the DNS Names in URLs for these services.

D) The continued support to collect and review system audit logs for the PKI solution.

E) The continued support required to obtain and provide annual PKI compliance audits until revocation of all issued certificates or the expiration of the longest-lived issued certificate.

iv) If the offeror is unable to abide by the Federal laws, ordinances, regulations, policies and/or agreements established with the FPKIPA, payment may be withheld by the ordering activity until they can be met. During this time the ordering activity may decide to accept the level of risk and require the offeror to continue providing PKI services so ordering activities can conduct day to day business and critical mission operations are not affected.

b) Description Of Authentication Products, Services And Pricing

i) Offerors shall provide a description of the PKI solution offered.

ii) PKI solutions shall be offered in accordance with standard commercial practice.

iii) Pricing shall be provided for the following shared infrastructure solution offered by the Contractor (does not include stand-alone IT Professional

Services):

A) A Certification Authority (CA) capable of issuing digital certificates and Certificate Revocation Lists (CRLs) compliant with COMMON;

B) A publicly accessible repository capable of hosting certificate validation artifacts (e.g., CA certificates and CRLs for retrieval);

C) Key management services such as private key escrow and recovery (to include third-party key recovery); and

D) Online Certificate Status Protocol (OCSP) validation services.

iv) If the following optional PKI components are required to operationalize the shared infrastructure solution, they may be offered on this SIN in conjunction with the above shared infrastructure solution:

A) A Registration Authority (RA) responsible for certificate issuance (to include identity proofing) and management in accordance with a Registration Practice Statement (RPS) compliant with COMMON.

B) A Card Management System (CMS) for the issuance and management of PIV credentials.

C) A Credential Management System for the issuance and management of Derived-PIV credentials.

SIN 561422 Automated Contact Center Solutions (ACCS)

561422 Automated Contact Center Solution (ACCS) is defined as any offering utilized to establish and maintain contact center capabilities for an agency. The offering may consist of one or more of the following: products, equipment, software, labor and/or services. Permissible offerings under this SIN may include any technologies or services required to deliver and support an ACCS for an agency, including but not limited to: Artificial Intelligence (AI), Chat Bots, Robotic Process Automation, Interactive Voice Response (IVR), Voice/Speech Recognition, Text-to-Speech, Voicemail, Callback, Web Callback, Email Delivery, Hosted Online Ordering, Hosted Email Web Form, Hosted FAQ Service, etc.

NOTE: Subject to Cooperative Purchasing

Cooperative Purchasing: Yes
Set Aside: No
FSC/PSC Code : DA01
Maximum Order : \$500,000

NAICS

Number	Description	Business Size
561422	Telmarketing Bureaus and Other contact Centers	\$25.5 million

Instructions:

Additional SIN Description: Automated services include, but not limited to Artificial Intelligence (AI), Chat Bots, Robotic Process Automation, Interactive Voice Response (IVR), Voice/Speech Recognition, Text-to-Speech, Voicemail, Callback, Web Callback, Email Delivery, Hosted Online Ordering, Hosted Email Web Form, Hosted FAQ Service, etc.).

IT Professional Services are included in this SIN.

Ancillary supplies and/or services shall neither be the primary purpose nor the preponderance of the work ordered, but be an integral part of the total solution offered.

1.) Specific Instructions for SIN 561422 - Automated Contact Center Solutions (ACCS)

a.) Transition Of Contact Center Services

i.) The time period required to transition from an ordering activity’s existing

contact center solution and requirements to new requirements (as defined in the task order), and shall be in accordance with the ordering activity's task order.

ii.) Transition shall begin at Notice-To-Proceed and continue for a period as specified in the task order. During the transition period, the Contractor shall work with the ordering activity to develop a sound project implementation plan and to perform all preparatory work to establish one or more fully functional multi-channel contact centers in support of the task.

iii.) The Government will transfer business and procedural data, including appropriate training material, to the Contractor, and work with the Contractor to establish appropriate system feeds.

iv.) The transition period will provide the Contractor with the opportunity to prepare and staff its contact center; develop the support of the knowledge base and scripts for automated response in support of the project; establish a fully functional contact center to handle the expected work volume; and complete all transition related activities to migrate the service to the new center.

v.) Based on the Contractor's ability and expert advice on transitioning the work volume, the ordering activity reserves the right to coordinate with the Contractor to achieve a staffing plan that minimizes disruption of the existing services and seamlessly transitions the customer base and work volumes to the new center.

F08. IT Training Subcategory

SIN 611420 Information Technology Training

611420 Includes training on hardware, software, cloud, and other applicable systems.

NOTE: Subject to Cooperative Purchasing

Cooperative Purchasing: Yes
Set Aside: No
FSC/PSC Code : U012
Maximum Order : \$250,000

NAICS

Number	Description	Business Size
611420	Computer Training	\$16 million

Instructions:

1) Specific Instructions for SIN 611420 – Information Technology Training

- a) Prepaid training tokens, credits, etc., shall not be permitted on this SIN.
- b) Offerors shall provide training courses normally available to commercial customers, which will permit ordering activity users to make full, efficient use of general purpose commercial IT products. Training is restricted to training courses for those products within the scope of the IT Category.
- c) Cancellation and Rescheduling
 - i) The ordering activity will notify the Contractor at least seventy-two (72) hours before the scheduled training date, if a student will be unable to attend. The Contractor will then permit the ordering activity to either cancel the order or reschedule the training at no additional charge. In the event the training class is rescheduled, the ordering activity will modify its original training order to specify the time and date of the rescheduled training class.
 - ii) In the event the ordering activity fails to cancel or reschedule a training course within the time frame specified above, the ordering activity will be liable for the contracted dollar amount of the

training course. The Contractor agrees to permit the ordering activity to reschedule a student who fails to attend a training class within ninety (90) days from the original course date, at no additional charge.

iii) The ordering activity reserves the right to substitute one student for another up to the first day of class.

iv) In the event the Contractor is unable to conduct training on the date agreed to by the Contractor and the ordering activity, the Contractor must notify the ordering activity at least seventy-two (72) hours before the scheduled training date.

d) Follow-Up Support

The Contractor agrees to provide each student with unlimited telephone support or online support for a period of one (1) year from the completion of the training course. During this period, the student may contact the Contractor's instructors for refresher assistance and answers to related course curriculum questions.

e) Format And Content Of Training

i) Offerors shall provide written materials (i.e., manuals, handbooks, texts, etc.) normally provided with course offerings, printed and copied two-sided on paper containing 30% postconsumer materials (fiber). Such documentation will become the property of the student upon completion of the training class.

ii) If applicable, for hands-on training courses, there must be a one-to-one assignment of IT equipment to students.

iii) Offerors shall provide each student with a Certificate of Training at the completion of each training course.

iv) Offerors shall provide the following information for each training course offered:

A) course title;

B) a brief description of the course content, to include the course format (e.g., lecture, discussion, hands-on training);

C) length of the course;

D) mandatory and desirable prerequisites for student enrollment;

E) minimum and maximum number of students per class;

F) locations where the course is offered;

G) class schedules; and

H) price (per student, per class (if applicable)).

v) For courses conducted at the ordering activity's location, instructor travel charges (if applicable), including mileage and daily living expenses (e.g., per diem charges) are governed by Pub. L. 99-234 and FAR Part 31.205-46, and are reimbursable by the ordering activity on orders placed under the Multiple Award Schedule, as applicable, in effect on the date(s) the travel is performed. The Industrial Funding Fee does NOT apply to travel and per diem charges.

vi) For Online Training Courses, a copy of all training material must be available for electronic download by the students.

f) "No Charge" Training

g) Offerors shall describe any training provided with equipment and/or software provided under this contract, free of charge as an attachment to the GSA Price List (I-FSS-600 CONTRACT PRICE LISTS (see current Solicitation for clause effective date)).

h) If other than the manufacturer, submit proof of authorization to provide training course(s) for manufacturer's software and/or hardware products.

F09. Telecommunications Subcategory

**Instructions:
Continuous Diagnostics and Mitigation (CDM) Approved Products**

GSA has partnered with the Cybersecurity and Infrastructure Security Agency (CISA) to showcase CISA approved CDM tools. The CISA CDM Program’s Approved Products List (APL) is the authoritative catalog for all approved CDM Tools and associated services. CDM APL Tools will carry the [CDM](#) tools symbol. The full complement of CDM subcategories includes tools, associated maintenance, and other related activities such as training. The CDM products and associated services undergo a DHS CISA product qualification process in order to be added to the CDM Approved Products List (APL). The APL features high-quality cybersecurity vendors offering products and related services to Federal, State, and Local Governments. CISA only accepts submissions to modify the CDM APL monthly. Offerors can submit updates to the APL on the first Monday of the first full or partial week of the month, with submissions being accepted through Friday of that week. A full submission calendar can be found on the CISA [website](#). For technical and CDM APL related questions, please contact the CISA CDM Program Office at csd_cb.acqbudg@cisa.dhs.gov.

SIN 517312 Wireless Mobility Solutions

517312 Wireless Mobility Solutions, including but not limited to, Wireless Carriers Services, Telecommunication Resellers, Other Mobility End-Point Infrastructure - Mobility infrastructure, Mobility-as-a-Service, Enterprise Mobility Management, Mobile Backend-as-a-Service, Telecom Expense Management, Mobile Application Vetting, Mobile Threat Protection, Mobile Identity Management, Internet of Things (IoT), and Other/Mobile Services.

All Nationwide Business Plans under this contract may include "no-cost" Service Enabling Devices (SEDs) (including, but not limited to, cell phones and shall be offered to the general public at "no-cost") and bundling the SEDs with cellular service. The SEDs are offered on an "as available" basis and may or may not be domestic end products or end products of a designated country. The "no-cost" SEDs are not available through this contract apart from ordering cellular service.

NOTE: Subject to Cooperative Purchasing

Cooperative Purchasing: Yes
Set Aside: No
FSC/PSC Code : DE11
Maximum Order : \$500,000

NAICS

Number	Description	Business Size
517112	WIRELESS TELECOMMUNICATIONS CARRIERS (EXCEPT SATELLITE)	1500 employees

Instructions:
 ****Best-in-Class (BIC) Designation****

Additional SIN Description: Includes a variety of services that address the mobility needs of government agencies. The following sub-categories associated with the Wireless & Mobile Services include but are not limited to:

1. Wireless Carrier Services (including, but not limited to, Wireless Telecommunications Carriers and Telecommunication Resellers of Wireless Services) which support mobile communications in CONUS and OCONUS locations
 - a. Voice Service plans and Features that enable mobile voice communications such as Voicemail, Three-way calling, etc.
 - b. Data Service plans and Features that provide connectivity and communications for data-capable mobile devices.

- c. Service Enabling Devices (SEDs) mobile devices bundled with voice and data service plans which are included at no cost to the ordering entity.
- d. Wireless infrastructure components (which do not include a service plan or features but may include labor) offered under a monthly lease arrangement or recurring charge to ordering entities.

2. Other Mobility End-Point Infrastructure - Mobility infrastructure

Includes mobile infrastructure equipment for implementing mobile solutions or enhancing wireless communications. Also includes user interfaces and miscellaneous hardware included with a mobile solution(s) or service.

3. Mobility-as-a-Service (MaaS)

A subscription-based, mobile management service suite enabling mobile endpoints, including SEDs to be managed, and utilized as a service. In this context a mobile endpoint is a user interface that requires wireless connectivity to communicate with an enterprise or carrier network. The service provider retains asset ownership of the endpoint(s) and provides service regarding asset issuance, endpoint performance management, service plan management, that mobility management software, and support services into a full solution that minimizes prior device-centric costs and operations. MaaS includes end-to-end management with respect to:

- a. Planning and Management of Agency MaaS Needs and Solutions
- b. Provisioning, Kitting, and Delivery
- c. Enterprise Mobility Management and SED Refresh
- d. Ongoing Helpdesk Support
- e. Logistics for end-of-life disposal / recycling

4. Enterprise Mobility Management (EMM)

Is a collective set of tools, software, and service capabilities required for the provision, management, security, and control of mobile device functionality, its applications, features and content that are delivered to government (or contractor) owned or employee owned (BYOD) mobile devices. The three main EMM areas include mobile device management (MDM), mobile application management (MAM), and mobility content management (MCM).

5. Mobile Backend-as-a-Service (MBaaS)

Represents mobile application delivery solutions that provide mobile application developers with a platform, tools, and libraries to develop, integrate, test and publish their applications to backend cloud storage and processing resources while also providing common features such as user management, push notifications, social networking integration, and other features demanded by mobile users.

6. Telecom Expense Management Services (TEMS)

Enterprise solutions which support the full lifecycle management of mobility and telecommunications assets. TEMS functions include cataloging, ordering, deployment, workflow management, inventory control, invoicing, disposition, and reporting of an enterprise's mobility resources. TEMS providers may offer standalone solutions and other support services, such as data and system integration services, to implement and maintain their solution

7. Mobile Application Vetting

Application Vetting or "app" vetting (also referred to as app threat intelligence or threat protection services) refers to software, processes, and tools required to test, validate, and verify mobile apps against a baseline of security, privacy, and organization-specific requirements and policies. Vendors may provide on premise, cloud-based, or outsourced app vetting solutions that run static and/or dynamic analysis tests and reporting on apps to detect security vulnerabilities and malicious or privacy violating behaviors.

8. Mobile Threat Protection (MTP)

MTP is a component of a layered Mobile Endpoint Protection Strategy that covers the major areas not addressed by EMM/MDM or App Vetting. MTP solutions monitor the mobile device in real-time to identify mobile threats that may compromise the device, mobile applications, or data residing on the device. MTP integrates with an EMM system deployed on devices resulting in

remediation or quarantining of the threat. The MTP solution evaluates an application threat and compliance against a set of pre-defined agency policies based upon acceptable risks, it validates operating system (OS) integrity against any compromise, it detects network threats such as MITM (Man-in-the-Middle) attacks and will detect device configuration risks.

9. Mobile Identity Management (MIM)

MIM is the secure integration of the attributes that unerringly identify a person in the physical and online environments, within the mobile device. MIM is a set of complementary products and solutions that issue and maintain certificates, which may include Derived PIV Credential (DPC) usage. A valid PIV card is required to issue a DPC. Once issued, credentials on a mobile device will support:

- a. Wifi authentication
- b. Virtual Private Networking
- c. User authentication to Commercial off the Shelf (COTS), Software-as-a-Service (SaaS), and other applications and services
- d. Data in Transit
- e. Data Encryption
- f. Signing of individual documents and records

10. Internet of Things (IoT)

Internet of Things (IoT) service providers engage with those who design, develop, operate or maintain an infrastructure of networked components comprised of computing resources, digital sensors, actuators, and human interfaces that are combined into systems to achieve specific goal(s).

11. Other/Mobile Services

Wireless communication services not commonly used across agency enterprises due to unique usage, features, niche application or legacy technology requirements. Examples include paging, short term rental/disposable endpoint component, and satellite-only communications providers.

Considerations for Wireless Carrier Services:

Telecommunications network service is one of several services excluded from the World Trade Organization (WTO) Government Procurement Agreement and the other Free Trade Agreement executed by the United States Government. See FAR 25.401(b).

Wireless service plans offered may include, at no-cost, Service Enabling Devices (SEDs) bundled together with the wireless service itself. A SED is a unit of, or directly associated with, contractor-provided and contractor-owned equipment used to meet the interface requirements for an individual service. A SED may also be a unit of, or directly associated with, contractor-provided and contractor-owned equipment or software used to enable the requirements associated with the services. The SEDs are not available through this contract apart from ordering the services under this SIN.

Specific Instructions for SIN 517312 - Wireless Mobility Solutions

- a) Acceptance Testing: Acceptance testing shall be performed of the systems for ordering activity approval in accordance with the approved test procedures.
- b) Equipment: Offerors shall make available cellular voice and data SEDs. The devices offered shall be compatible with the cellular access standards employed within the geographical scope of contract. Offerors shall provide programming of any cellular telephone device, including offeror-provided and ordering activity-furnished devices, that conforms to the cellular service furnished by the Offeror.
- c) Management & Operations - Pricing: In accordance with standard commercial practice, the offeror shall provide installation, operation, maintenance, and engineering interface training on the system.
- d) Contract Level Program Reporting Requirement: In accordance with standard commercial practice, the offeror may provide a monthly/quarterly summary ordering activity report.

Enhanced Reporting Requirement for services under subcategory ONE (1) - WIRELESS

CARRIER SERVICES - The Agency Billing Summary Report (ABSR) data reporting requirement will be achieved via a bilateral modification.

The Enhanced Reporting requirement described herein is specific to SIN 517312 - Wireless Mobility Solutions and is in addition to and not in lieu of the <https://srp.fas.gsa.gov/> reporting procedures. SIN 517312 - Wireless Mobility Solutions requires the following mandatory reporting requirements in order for GSA to maintain OMB's "Best-in-Class" (BIC) designation in Federal contract <https://srp.fas.gsa.gov/s> for Wireless Services. The BIC designation was achieved for the FSSI Program, in large part, due to the ability to gather and improve the Agency Summary Billing Report (ASBR) data reporting from FSSI Wireless (FSSI-W) contractors. Cooperation with the major carriers over the past three years has enabled GSA to improve the timeliness and quality <https://srp.fas.gsa.gov/> of reporting, but also reduce burden to industry by automating various processes.

Offerors providing ABSR reporting for Wireless Carrier Services will be required to submit reporting in accordance with the following data elements. As practiced through the current FSSI-W program, vendors will submit their ABSR reports through the existing GSA TSC Reporting Portal (<https://tscportal.fas.gsa.gov/#/login>).

- Account Name
- Account Number
- CLIN
- Item Description
- Quantity of Units
- Unit Price
- Billed Monthly Recurring Charge
- Prorated MRC (Y/N)
- Usage Non-Recurring Charge (NRC)
- Non-Usage NRC
- Adjustments/Credits
- Taxes/Surcharges
- Agency Fee
- Subtotal
- Account Total
- Post Billing Charge (\$)
- Task Order > \$150k (Y/N)
- Comments

All offerors shall be expected to report their Total Invoice Amounts for each Fiscal Year Quarter. Furthermore, offerors shall report sales results specifying the subcategory or the sub-categories of Wireless Carrier Services, Telecom Expense Management, Enterprise Mobility Management, Mobility Identity Management, Mobile Threat Protection, and Mobility-as-a-Service. Offerors shall report the estimated number of units sold in conjunction with their Total Invoiced Amount. The following table summarizes the reporting requirements required by the program for each mobile services subcategory:

e) Wireless Service Plans

- i) The following shall be included as an attachment to the GSA Price List (I-FSS-600 CONTRACT PRICE LISTS (see current Solicitation for clause effective date)).
- ii) Describe the wireless service plan and eligibility requirements. Including,

but not limited to, service area, monthly service charge, minutes included, etc.

iii) Describe charges, if any, for additional minutes, domestic wireless long distance, roaming, nights and weekends, etc.

iv) Describe corporate volume discounts and eligibility requirements, if any.

12. SIN Subgroups: Upon completion of the technical evaluation for both offers and modifications, the government will determine which of the following 11 SIN subgroups apply to the subject offer:

1. Wireless Carrier Services
2. Mobility Infrastructure
3. Mobility-as-a-Service (MaaS)
4. Enterprise Mobility Management (EMM)
5. Mobile Backend-as-a-Service (MBaaS)
6. Telecom Expense Management (TEM)
7. Mobile Application Vetting
8. Mobile Threat Protection (MTP)
9. Mobile Identity Management
10. Internet of Things (IoT)
11. Other/Mobile Services

Following notification that they are eligible for one or more of the 5 SIN subgroups, awarded contractors may select the corresponding subgroups by following the instructions below:

1. Login to eBuy
2. From the top menu, select "Profile"
3. Click "Modify Subgroups"
4. Select the applicable subgroups according to the instructions

All contractor selections will be monitored by GSA for compliance and action will be taken against your contract if you select Subgroups that have not been awarded under your contract.

SIN 517410 Commercial Satellite Communications Solutions (COMSATCOM)

517410 Includes but not limited to products and services, such as: leased commercially available satellite bandwidth; shared or private satellite subscription/managed services; satellite phone services; satellite terminals, phones, modems, and related equipment and services. Solutions include transponded capacity consisting of dedicated bandwidth on a commercial satellite in any frequency band. Transponded Capacity includes all services necessary to allow the customer to use the transponded capacity, including: engineering (e.g., development of link budgets, transmission plans); basic customer training (e.g., acquiring satellite signal, peak and polarization); core management and control of the transponded capacity; and required approvals. Subscription Services include but are not limited to: worldwide satellite-based Internet, voice, data, and video services. Subscription services entail existing commercial satellite services solutions, including terminals, in any frequency band. Subscription services include the network management, monitoring, engineering, integration, and operations required to deliver the services. These solutions may include fixed and/or mobile satellite services, along with service-enabling components such as terminals, teleports, and terrestrial interfaces. Host Nation Agreements (HNAs) are separately priced when required.

NOTE: Subject to Cooperative Purchasing

Cooperative Purchasing: Yes
Set Aside: No
FSC/PSC Code : DG11
Maximum Order : \$500,000

NAICS

Number	Description	Business Size
517410	Satellite Telecommunications	\$44 million

Instructions:

****Best-in-Class (BIC) Designation****

1) Specific Instructions for SIN 517410 - Commercial Satellite Communications Solutions (COMSATCOM)

a) Flexibility/Optimization: Flexibility/optimization/re-grooming allows the Offeror to redistribute resources currently used to provide COMSATCOM Services (example: space segment, network, teleport, terminal resources) or customers sharing the COMSATCOM Services resources (example: customer one with typical peak usage at 9:00 a.m. and customer two with typical peak usage at 3:30 p.m.), enabling the Ordering Activity to gain spectral, operational, and/or price efficiencies.

b) Network Monitoring (Net Ops): Offerors shall be capable of collecting and delivering near real-time monitoring, fault/incident/outage reporting, and information access required to ensure effective and efficient operations, performance, and availability consistent with commercial best practices. Ordering activities may propose additional terms and conditions within the requirement (example: specific predefined terms and conditions for Net Ops collection and delivery.) However, if the supplemental terms and conditions contradict the contract, the contract takes precedence.

c) EMI/RFI Identification, Characterization, AND GEO-Location: When the ordering activity requires Electro Magnetic Interference (EMI) / Radio Frequency Interference (RFI) identification, characterization, and geo-location, the offeror shall provide a mutually agreed upon media and voice communications capability capable of protecting "Sensitive, but Unclassified" data.

d) Description of COMSATCOM Services And Pricing

i) The following shall NOT be included on the GSA Price List (I-FSS-600 CONTRACT PRICE LISTS (see current Solicitation for clause effective date)).

ii) Description of COMSATCOM Transponded Capacity and Pricing

- Proposed prices shall show Bandwidth ranges (example: 0 - 4.5 MHz, 4.5 – 9.0 MHz, etc.), unit price and region (example: North America, Africa). NOTE: If pricing is for different time periods (example: day, week, month, or year) provide that information.
- Suggestion: Use regions instead of satellite names to reduce the number of contract modifications.
- If applicable, provide at least one Worldwide Host Nation Agreement (HNA) description and ceiling price.
- If applicable, price other non-standard required licenses and agreements in the same manner as HNAs.
- Provide sufficient performance metrics for the offered COMSATCOM transponded capacity services to ensure proper delivery of service. Metrics examples: service availability (example: 97.5%, 99.5%), grade of service, minimum service levels, quality of service, time to restore service, etc.
- Indicate price inclusions and exclusions for each priced service (example: portability, re- grooming, etc.).
- Description of services and prices shall include all services necessary to use the transponded capacity, including: limited engineering (example: development of link budgets, transmission plans); basic customer training (example: acquiring satellite signal, peak and polarization); core management and control of the transponded capacity; and required approvals (example: frequency clearances, landing rights).

iii) Description of COMSATCOM Subscription Services and Pricing

- If applicable, provide third party billing service description with a ceiling price (example: per megabyte price, per minute price).

- Describe Fixed Satellite Subscription Services by regions, bandwidth ranges, data rate ranges, per unit pricing and/or flat rate service packages, when applicable.
- Identify oversubscription rates, standard quality of service (QoS) profiles, and service availability targets.
- Describe Mobile Satellite Subscription Services in the standard commercial format (i.e., per unit pricing and/or flat rate service packages, etc.)
- If applicable, describe and price non-recurring charges (example: service activation).
- The Government reserves the right to use Government Furnished Access Point Names (APN) for remote user access into Government user networks and enclaves instead of using those provided by Offerors. Offeror should describe and separately price value added services that can be used in conjunction with Government Furnished APNs.
- Equipment provided as part of the Subscription Services is acceptable. NOTE: Equipment can be leased or purchased through the IT Equipment Subcategory SINs.
- Offeror shall provide sufficient performance metrics for the offered COMSATCOM subscription services to ensure proper delivery of service. Metrics examples: service availability, grade of service, minimum service levels, quality of service, time to restore service, etc.
- Indicate price inclusions and exclusions for each priced service (example: portability, regrooming, committed information rates (CIR), etc.).
- Description of services and prices shall include all services necessary to use the Subscription Services, including: network management, monitoring, engineering, integration, and operations required to deliver the services.

iv) Portability Examples

- Description of portability may include moving from one transponder/satellite to another, one managed service area to another, transponded capacity redeployment between beams or transponders on a single satellite, redeployment from one frequency band to another, physical relocation of a satellite to a new orbital position, re-routing of teleports services from one teleport to another predefined teleport, re-routing of traffic from one terrestrial infrastructure to another predefined infrastructure, and movement of Network Operations Center (NOC) services from one NOC to another NOC.

v) Network Monitoring (Net Ops) and Reporting

- Describe Net Ops services available for monitoring and reporting such as spectrum sweep results, transponder status, radio frequency (RF) gateway (teleport) status, network outage, degraded service, reduced data rates, packet loss, and any element of the service offering that could result in a customer service affecting condition.
- Describe the electronic formats available for information access by the Ordering Activity (example: XML, SNMP traps, etc.)
- Offeror shall establish and provide to each Ordering Activity and to customers on a requirement basis how they will communicate fault/incident/outage information to customers including toll free phone numbers, WebPages, email to distribution lists, etc.

e) Contract Level Program Reporting Requirement

i) 517410 - Commercial Satellite Communications Solutions (COMSATCOM) awarded task order specific information shall be submitted on a quarterly basis.

ii) This reporting requirement is for all awards made after SIN 517410 - Commercial Satellite Communications Solutions (COMSATCOM) was added to the MAS contract. This includes BPA's without existing orders.

iii) The report template provided by GSA shall be used. A copy of the reporting template is

available from the GSA Contract Specialist or contracting officer assigned to your contract.

iv) The quarterly report shall contain:

A) Vendor Information

- Vendor Name
- Vendor Contract Number

B) Customer Information

- Agency Name Ordering Activity City
- State
- Zip Code
- Contracting Officer Name
- Contracting Officer Phone Number
- Contracting Officer Email

C) Order Information

- Date of Order Order Number
- Modification Number Requisition Number Description of Services
- Period of Performance Start Date Period of Performance End Date Total Order Value
- SIN Number: SIN 517410 - Commercial Satellite Communications Solutions (COMSATCOM)
- Line Item Description
- Quantity Sold Unit o Unit Price Extended Price Frequency Band
- Bandwidth Capacity Data Rate
- Regional Coverage Satellite Name or Number
- MAC Requirement (Security Level I, II, or III) Private or Shared Network
- HNA Requirement (Y/N) Portability Service (Y/N) Expedited Delivery (Y/N) Commercial Teleport (Y/N)

D) The quarterly report is due NLT 15 days after the end of each FY quarter.

E) Quarterly report shall be submitted using the GSA SATCOM Report Portal. The URL and information on how to access the portal will be provided by the GSA SATCOM PMO.

SIN Level Regulations:

Regulation Number	Regulation Title/Comments
552.238-110	COMMERCIAL SATELLITE COMMUNICATION (COMSATCOM) SERVICES (MAY 2023)

Full Text Regulations:

Begin Regulation

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) (DEVIATION NOV 2025)

(a) The offeror must check the following certification:

Certification

The offeror # does # does not certify that-

(1) The items of equipment to be serviced under this contract are used regularly for other than Government purposes, and are sold or traded by the offeror (or subcontractor in the case of an exempt subcontractor) in substantial quantities to the general public in the course of normal business operations;

(2) The services will be furnished at prices which are, or are based on, established catalog or market prices for the maintenance, calibration, or repair of equipment.

(i) An "established catalog price" is a price included in a catalog, price list, schedule, or other form that is regularly maintained by the manufacturer or the offeror, is either published or otherwise available for inspection by customers, and states prices at which sales currently, or were last, made to a significant number of buyers constituting the general public.

(ii) An "established market price" is a current price, established in the usual course of trade between buyers and sellers free to bargain, which can be substantiated from sources independent of the manufacturer or offeror; and

(3) The compensation (wage and fringe benefits) plan for all service employees performing work under the contract are the same as that used for these employees and equivalent employees servicing the same equipment of commercial customers.

(b) Certification by the offeror as to its compliance with respect to the contract also constitutes its certification as to compliance by its subcontractor if it subcontracts out the exempt services. If the offeror certifies to the conditions in paragraph (a) of this provision, and the Contracting Officer determines in accordance with FAR 22.1002-1(e)(3) that the Service Contract Labor Standards statute-

(1) Will not apply to this offeror, then the Service Contract Labor Standards clause in this solicitation will not be included in any resultant contract to this offeror; or

(2) Will apply to this offeror, then the clause at [52.222-51](#), Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements, in this solicitation will not be included in any resultant contract awarded to this offeror, and the offeror may be provided an opportunity to submit a new offer on that

basis.

(c) If the offeror does not certify to the conditions in paragraph (a) of this provision-

(1) The clause in this solicitation at [52.222-51](#), Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements, will not be included in any resultant contract awarded to this offeror; and

(2) The offeror must notify the Contracting Officer as soon as possible, if the Contracting Officer did not attach a Service Contract Labor Standards wage determination to the solicitation.

(d) The Contracting Officer may not make an award to the offeror, if the offeror fails to execute the certification in paragraph (a) of this provision or to contact the Contracting Officer as required in paragraph (c) of this provision.

(End of provision)

Begin Regulation

52.229-1 STATE AND LOCAL TAXES (APR 1984)

Notwithstanding the terms of the Federal, State, and Local Taxes clause, the contract price excludes all State and local taxes levied on or measured by the contract or sales price of the services or completed supplies furnished under this contract. The Contractor shall state separately on its invoices taxes excluded from the contract price, and the Government agrees either to pay the amount of the taxes to the Contractor or provide evidence necessary to sustain an exemption.

Begin Regulation

552.238-107 TRAFFIC RELEASE (SUPPLIES) (MAY 2019)

Supplies ordered by GSA for export will not be shipped by the Contractor until shipping instructions are received from GSA. To obtain shipping instructions, the Contractor shall forward completed copies of GSA Form 1611, Application for Shipping Instructions and Notice of Availability, to the GSA office designated on the purchase order at least 15 days prior to the anticipated shipping date. Copies of GSA Form 1611 will be furnished to the Contractor with the purchase order. Failure to comply with this requirement could result in nonacceptance of the material by authorities at the port of exportation. When supplies for export are ordered by other Government agencies the Contractor should obtain shipping instructions from the ordering agency.

Begin Regulation

552.238-73 IDENTIFICATION OF ELECTRONIC OFFICE EQUIPMENT PROVIDING ACCESSIBILITY FOR INDIVIDUALS WITH DISABILITIES (MAR 2022)

(a) Definitions.

"Electronic office equipment accessibility" means the application/configuration of electronic office equipment (includes hardware, software and firmware) in a manner that accommodates the functional limitations of individuals with disabilities so as to promote productivity and provide access to work related and/or public information resources.

"Individuals with Disabilities" mean qualified individuals with impairments as cited in 29 U.S.C. 705(20) who can benefit from electronic office equipment accessibility.

"Special peripheral" means a special needs aid that provides access to electronic equipment that is otherwise inaccessible to individuals with disabilities.

(b) The offeror is encouraged to identify in its offer, and include in any commercial catalogs and pricelists accepted by the Contracting Officer, office equipment, including any special peripheral, that will facilitate electronic office equipment accessibility for individuals with disabilities. Identification should include the type of disability accommodated and how the users with that disability would be helped.

End of clause

Begin Regulation

552.238-89 DELIVERIES TO THE U.S. POSTAL SERVICE (MAY 2019)

(a) *Applicability.* This clause applies to orders placed for the U.S. Postal Service (USPS) and accepted by the Contractor for the delivery of supplies to a USPS facility (consignee).

(b) *Mode/method of transportation.* Unless the Contracting Officer grants a waiver of this requirement, any shipment that meets the USPS requirements for mailability (i.e., 70 pounds or less, combined length and girth not more than 108 inches, etc.) delivery shall be accomplished via the use of the USPS. Other commercial services shall not be used, but this does not preclude the Contractor from making delivery by the use of the Contractor's own vehicles.

(c) *Time of delivery.* Notwithstanding the required time for delivery to destination as may be specified elsewhere in this contract, if shipments under this clause are mailed not later than five (5) calendar days before the required delivery date, delivery shall be deemed to have been made timely.

Begin Regulation

552.238-90 CHARACTERISTICS OF ELECTRIC CURRENT (MAY 2019)

Contractors supplying equipment which uses electrical current are required to supply equipment suitable for the electrical system at the location at which the equipment is to be used as specified on the order.

Begin Regulation

552.238-91 MARKING AND DOCUMENTATION REQUIREMENTS FOR SHIPPING (MAY 2019)

(a) *Responsibility.* It shall be the responsibility of the ordering activity to determine the full marking and documentation requirements necessary under the various methods of shipment authorized by the contract.

(b) *Documentation.* In the event the ordering activity fails to provide the essential information and documentation, the Contractor shall, within three days after receipt of order, contact the ordering activity and advise them accordingly. The Contractor shall not proceed with any shipment requiring transshipment via U.S. Government facilities without the prerequisites stated in paragraph (c) of this

section.

(c) *Direct shipments*. The Contractor shall mark all items ordered against this contract with indelible ink, paint or fluid, as follows:

- (1) Traffic Management or Transportation Officer at FINAL destination.
- (2) Ordering Supply Account Number.
- (3) Account number.
- (4) Delivery Order or Purchase Order Number.
- (5) National Stock Number, if applicable; or Contractor's item number.
- (6) Box _____ of _____ Boxes.
- (7) Nomenclature (brief description of items).

Begin Regulation

**552.238-92 VENDOR MANAGED INVENTORY (VMI) PROGRAM
(MAY 2019)**

(a) The term "Vendor Managed Inventory" describes a system in which the Contractor monitors and maintains specified inventory levels for selected items at designated stocking points. VMI enables the Contractor to plan production and shipping more efficiently. Stocking points benefit from reduced inventory but steady stock levels.

(b) Contractors that commercially provide a VMI-type system may enter into similar partnerships with ordering agencies under a Blanket Purchase Agreement.

Begin Regulation

552.238-93 ORDER ACKNOWLEDGMENT (MAY 2019)

Contractors shall acknowledge only those orders which state "Order Acknowledgment Required." These orders shall be acknowledged within 10 calendar days after receipt. Such acknowledgment shall be sent to the ordering activity placing the order and contain information pertinent to the order, including the anticipated delivery date.

Begin Regulation

**552.238-94 ACCELERATED DELIVERY REQUIREMENTS (MAY
2019)**

When the Federal Supply Schedule contract delivery period does not meet the bona fide urgent delivery requirements of an ordering activity, the ordering activity is encouraged, if time permits, to contact the Contractor for the purpose of obtaining accelerated delivery. The Contractor shall reply to the inquiry within three (3) business days 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.

Begin Regulation

552.238-81 PRICE REDUCTIONS (DEC 2021) (DEVIATION)

- (a) Before award of a contract, the Contracting Officer and the Offeror will agree upon (1) the customer (or category of customers) which will be the basis of award, and (2) the Government's price or discount relationship to the identified customer (or category of customers). This relationship shall be maintained throughout the contract period. Any change in the Contractor's commercial pricing or discount arrangement applicable to the identified customer (or category of customers) which disturbs this relationship shall constitute a price reduction.
- (b) During the contract period, the Contractor shall report to the Contracting Officer all price reductions to the customer (or category of customers) that was the basis of award. The Contractor's report shall include an explanation of the conditions under which the reductions were made.
- (c)(1) A price reduction shall apply to purchases under this contract if, after the date negotiations conclude, the Contractor—
- (i) Revises the commercial catalog, pricelist, schedule or other document upon which contract award was predicated to reduce prices;
 - (ii) Grants more favorable discounts or terms and conditions than those contained in the commercial catalog, pricelist, schedule or other documents upon which contract award was predicated; or
 - (iii) Grants special discounts to the customer (or category of customers) that formed the basis of award, and the change disturbs the price/discount relationship of the Government to the customer (or category of customers) that was the basis of award.
- (2) The Contractor shall offer the price reduction to the eligible ordering activity with the same effective date, and for the same time period, as extended to the commercial customer (or category of customers).
- (d) There shall be no price reduction for sales—
- (1) To commercial customers under firm, fixed-price definite quantity contracts with specified delivery in excess of the maximum order threshold specified in this contract;
 - (2) To Federal agencies;
 - (3) Made to Eligible Ordering Activities identified in GSAR Clause 552.238-113 when the order is placed under this contract (and the Eligible Ordering Activities identified in GSAR Clause 552.238-113 is the agreed upon customer or category of customer that is the basis of award); or
 - (4) Caused by an error in quotation or billing, provided adequate documentation is furnished by the Contractor to the Contracting Officer.[or;
 - (5) Cloud computing services offered on a consumption basis under Special Item Number (SIN) 518210C (previously 132-40) or successor SINs within the Information Technology (IT) Category (previously Schedule 70).]
- (e) The Contractor may offer the Contracting Officer a voluntary Governmentwide price reduction at any time during the contract period.
- (f) The Contractor shall notify the Contracting Officer of any price reduction subject to this clause as soon as possible, but not later than 15 calendar days after its effective date.
- (g) The contract will be modified to reflect any price reduction which becomes applicable in accordance with this clause.

(End of clause)

Begin Regulation

552.238-199 SPECIAL ORDERING PROCEDURES APPLICABLE WHEN PROCURING CLOUD COMPUTING ON A CONSUMPTION BASIS (MAR 2022)

- (a) Definitions.
- (1) "Capital asset" has the meaning given the term by Office of Management and Budget (OMB) Circular A-11 Capital Programming Guide and any amendatory or superseding document(s) thereto.
 - (2) "Cloud computing" has the meaning given the term by the National Institute of Standards and Technology in Special Publication (SP) 800-145 and any amendatory or superseding document(s) thereto.
 - (3) "Consumption basis" or "consumption-based" means any offering that is metered with charges that accrue on a predetermined periodic basis (e.g., per second, minute, hour, week, month, or

another per-unit basis) and is billed based on actual usage during an elapsed period with predetermined pricing or discounts.

(4) "Requirements task order" means a task order that provides for filling all actual purchase requirements of a designated Ordering Activity during a specified contract period, with performance by the Contractor being scheduled when the Ordering Activity awards, or exercises options for, individual contract line items (CLINs) under the task order.

(i) This task order type is appropriate when the Ordering Activity anticipates recurring requirements but cannot predetermine the precise quantities of services that it will need during a definite period.

(ii) A requirements task order issued under a FSS contract is a single contract award as defined FAR 2.101. Individual CLINs executed and funded under this task order type are not considered to be second-tier instruments issued under the awarded task order.

(iii) A requirements task order is not a requirements contract as described at FAR 16.503.

(b) Ordering procedures.

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

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

(c) Applicability.

(1) The Ordering Activity Contracting Officer shall follow the procedures contained within this clause when placing an incrementally funded task order under this contract for cloud computing services on a consumption basis.

(2) The Ordering Activity Contracting Officer is permitted, but not required to use the procedures contained within this clause for task orders that are not incrementally funded.

(3) The Ordering Activity Contracting Officer shall not use the procedures contained within this clause for the acquisition, maintenance, or modification of capital assets.

(d) Pricing.

(1) The Ordering Activity Contracting Officer shall establish a task order ceiling price for all estimated requirements.

(2) All cloud computing services offered under this FSS contract are considered fixed-price.

(e) Task order type.

The Ordering Activity Contracting Officer shall use a requirements task order for cloud computing services procured on a consumption basis in accordance with this clause.

(1) This task order type may include other contract types, such as firm-fixed-price, when procuring other offerings under this contract that are not being procured on a consumption-basis.

(2) Estimates for cloud computing services to be procured on a consumption basis.

(i) The Ordering Activity Contracting Officer must state a realistic estimate of—

(A) The consumption of cloud computing services in the task order solicitation;
and

(B) The total amount in dollars to be expended on cloud consumption in the task order.

(ii) This estimate is not a representation to an Offeror or Contractor that the estimated consumption will be required or ordered, or that conditions affecting requirements will be stable or normal.

(iii) The Ordering Activity Contracting Officer may obtain the estimate from records of previous requirements and consumption, or by other means, and should base the estimate on the most current information available.

(iv) If the Government's requirements do not meet this estimate, that fact shall not constitute the basis for an equitable price adjustment.

(3) All CLINs within the task order must include a defined scope with all services priced at the time of award.

(f) Incremental funding.

(1) The Ordering Activity may allot funds incrementally as the bona fide need arises for predefined and established fixed-priced procurement requirements on individual CLINs.

(2) The Ordering Activity shall ensure sufficient funds are allotted to the task order—

(i) At the time of award to cover the total amount payable to the Contractor for the

- awarded CLIN(s); and
- (ii) At the time an optional CLIN is exercised to cover the total amount payable to the Contractor for that optional CLIN.
- (3) Nothing in this clause shall be construed to supersede the Ordering Activity's contract funding policies.
- (g) Consumption monitoring.
- (1) The Contractor shall—
- (i) Provide, at no additional cost to the Government, access to tools that enable the Government to track its usage of cloud computing services offered on a consumption basis; or
- (ii) Notify the Ordering Activity Contracting Officer when total consumption reaches—
- (A) 50 percent and 75 percent of the ceiling price for each CLIN for consumption-based cloud computing services, or other milestones as agreed upon by the Contractor and the Ordering Activity Contracting Officer; and
- (B) 50 percent and 75 percent of the task order ceiling price, or other milestones as agreed upon by the Contractor and the Ordering Activity Contracting Officer.
- (2) The Ordering Activity Contracting Officer shall determine that the consumption monitoring capabilities offered by the Contractor will enable the Government to adequately track its incurred costs before awarding a task order in accordance with this clause.
- (h) Limitation of funds.
- (1) The Government will not be obligated to pay the Contractor any amount in excess of the ceiling price in the task order, and the Contractor shall not be obligated to continue performance if doing so would exceed the ceiling price set forth in the task order.
- (2) The Ordering Activity Contracting Officer may use a Limitation of Funds clause when CLINs under the task order are incrementally funded.
- (i) Scope reviews.
- (1) The Ordering Activity Contracting Officer is encouraged to request a scope review from the GSA Federal Acquisition Service (FAS) Office of Information Technology Category (ITC) before placing a task order in accordance with these special ordering procedures.
- (2) The purpose of a scope review is to analyze whether the planned acquisition is—
- (i) compatible with the scope of Special Item Number (SIN) 518210C (previously 132-40) or successor SINs;
- (ii) utilizing recommended best practices; and
- (iii) not for the acquisition, maintenance, or modification of capital assets.
- (3) The Ordering Activity Contracting Officer may request a scope review by contacting FAS ITC at cloud-sin-rfi@gsa.gov.

(End of Clause)

Begin Regulation

52.207-5 OPTION TO PURCHASE EQUIPMENT (FEB 1995)

- (a) The Government may purchase the equipment provided on a lease or rental basis under this contract. The Contracting Officer may exercise this option only by providing a unilateral modification to the Contractor. The effective date of the purchase will be specified in the unilateral modification and may be any time during the period of the contract, including any extensions thereto.
- (b) Except for final payment and transfer of title to the Government, the lease or rental portion of the contract becomes complete and lease or rental charges shall be discontinued on the day immediately preceding the effective date of purchase specified in the unilateral modification required in paragraph (a) of this clause.
- (c) The purchase conversion cost of the equipment shall be computed as of the effective date specified in the unilateral modification required in paragraph (a) of this clause, on the basis of the purchase price set forth in the contract, minus the total purchase option credits accumulated during the period of lease or rental, calculated by the formula contained elsewhere in this contract.

(d) The accumulated purchase option credits available to determine the purchase conversion cost will also include any credits accrued during a period of lease or rental of the equipment under any previous Government contract if the equipment has been on continuous lease or rental. The movement of equipment from one site to another site shall be “continuous rental.”

Begin Regulation

**552.238-109 AUTHENTICATION SUPPLIES AND SERVICES
(MAY 2019)**

(a) *General background.* (1) The General Services Administration (GSA) established the “Identity and Access Management Services” (IAMS) Program to clearly define the kinds of digital certificates and PKI services that meet the requirements for service providers and supplies that support FISMA-compliant IAM systems deployed by Federal agencies.

(2) Homeland Security Presidential Directive 12 (HSPD-12), “Policy for a Common Identification Standard for Federal Employees and Contractors” establishes the requirement for a mandatory Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and Contractor employees assigned to Government contracts in order to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. Further, the Directive requires the Department of Commerce to promulgate a Federal standard for secure and reliable forms of identification within six months of the date of the Directive. As a result, the National Institute of Standards and Technology (NIST) released Federal Information Processing Standard (FIPS) 201-2: Personal Identity Verification of Federal Employees and Contractors August 2013. FIPS 201-2 requires that the digital certificates incorporated into the Personal Identity Verification (PIV) identity credentials comply with the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework. In addition, FIPS 201-2 requires that Federal identity badges referred to as PIV credentials, issued to Federal employees and Contractors comply with the Standard and associated NIST Special Publications 800-73, 800-76, 800-78, and 800-79.

(b) *Special item numbers.* GSA has established the e-Authentication Initiative (see URL: <http://www.idmanagement.gov>) to provide common infrastructure for the authentication of the public and internal Federal users for logical access to Federal e-Government applications and electronic services. To support the government-wide implementation of HSPD-12 and the Federal e-Authentication Initiative, GSA has established Special Item Numbers (SINs) pertaining to Authentication Products and Services, including Electronic Credentials, Digital Certificates, eAuthentication, Identify and Access Management, PKI Shared Service Providers, and HSPD-12 Product and Service Components.

(c) *Qualification information.*

(1) All Authentication supplies and services must be qualified as being compliant with Government-wide requirements before they will be included on a GSA Information Technology (IT) Schedule contract. The Qualification Requirements and associated evaluation procedures against the Qualification Requirements for each SIN and the specific Qualification Requirements for HSPD-12 implementation components are presented at the following URL: <http://www.idmanagement.gov>.

(2) In addition, the National Institute of Standards and Technology (NIST) has established the NIST Personal Identity Verification Program (NPIVP) to evaluate integrated circuit chip cards and supplies against conformance requirements contained in FIPS 201. GSA has established the FIPS 201 Evaluation Program to evaluate other supplies needed for agency implementation of HSPD-12 requirements where normative requirements are specified in FIPS 201 and to perform card and reader interface testing for interoperability. Products that are approved as FIPS-201 compliant through these evaluation and testing programs may be offered directly through HSPD-12 Supplies and Services Components SIN under the category “Approved FIPS 201-Compliant Products and services.”

(d) *Qualification requirements.* Offerors proposing Authentication supplies and services under the established SINs are required to provide the following:

(1) Proposed items must be determined to be compliant with Federal requirements for that SIN. Qualification Requirements and procedures for the evaluation of supplies and services are posted at the URL: <http://www.idmanagement.gov>. GSA will follow these procedures in qualifying offeror's supplies and services against the Qualification Requirements for applicable to SIN. Offerors must submit all documentation certification letter(s) for Authentication Supplies and Services offerings at the same time as submission of proposal. Award will be dependent upon receipt of official documentation from the Acquisition Program Management Office (APMO) listed below verifying satisfactory qualification against the Qualification Requirements of the proposed SIN(s).

(2) After award, Contractor agrees that certified supplies and services will not be offered under any other SIN on any Federal Supply Schedule

(3) (i) If the Contractor changes the supplies or services previously qualified, GSA may require the Contractor to resubmit the supplies or services for re-qualification.

(ii) If the Federal Government changes the qualification requirements or standards, Contractor must resubmit the supplies and services for re-qualification.

(4) Immediately prior to making an award, Contracting Officers MUST consult the following website to ensure that the supplies and/or services recommended for award under any Authentication Supplies and Services SINs are in compliance with the latest APL qualification standards: www.idmanagement.gov. A dated copy of the applicable page should be made and included with the award documents.

(e) *Demonstrating conformance.*

(1) The Federal Government has established Qualification Requirements for demonstrating conformance with the Standards. The following websites provide additional information regarding the evaluation and qualification processes

(i) For Identify and Access Management Services (IAMS) and PKI Shared Service Provider (SSP) Qualification Requirements and evaluation procedures: <http://www.idmanagement.gov>;

(ii) For HSPD-12 Product and Service Components Qualification Requirements and evaluation procedures: <http://www.idmanagement.gov>;

(iii) For FIPS 201 evaluation program testing and certification procedures: <https://www.idmanagement.gov/fips201/>.

(f) *Acquisition Program Management Office (APMO).* GSA has established the APMO to provide centralized technical oversight and management regarding the qualification process to industry partners and Federal agencies. Contact the following APMO for information on the eAuthentication Qualification process. Technical, APMO, FIPS 201, and HSPD-12 Points of Contact can be found below, or in an additional attachment to the solicitation.

[The contracting officer should insert the points of contact information below, unless otherwise included elsewhere in the solicitation.]

SownerInsert1

Begin Regulation

**552.238-110 COMMERCIAL SATELLITE COMMUNICATION
(COMSATCOM) SERVICES (MAY 2023)**

(a) *General background.* A Special Item Number (SIN) has been established for Commercial Satellite Communications (COMSATCOM) services, focused on transponded capacity and fixed and mobile subscription services, to make available common COMSATCOM services to all Ordering Activities.

(b) *Information assurance.*

(1) The Contractor shall demonstrate, to the maximum extent practicable, the ability to meet:

(i) The Committee on National Security Systems Policy (CNSSP) 12, "National Information Assurance Policy for Space Systems used to Support National Security Missions," or

(ii) Department of Defense Directive (DoDD) 8581.1, "Information Assurance (IA) Policy for Space Systems Used by the Department of Defense."

(2) The Contractor shall demonstrate the ability to comply with the Federal Information Security Management Act of 2002 as implemented by Federal Information Processing Standards Publication 200 (FIPS 200), "Minimum Security Requirements for Federal Information and Information Systems." In response to ordering activity requirements, at a minimum, all services shall meet the requirements assigned against:

(i) A low-impact information system (per FIPS 200) that is described in the current revision of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," or

(ii) A Mission Assurance Category (MAC) III system that is described in the current revision of DoD Instruction (DoDI) 8500.2, "Information Assurance Implementation."

(3) The Contractor's information assurance boundary is where the Contractor's services connect to the user terminals/equipment (i.e., includes satellite command encryption (ground and space); systems used in the Satellite Operations Centers (SOCs), Network Operations Centers (NOCs) and teleport; and terrestrial infrastructure required for service delivery).

(c) *Delivery schedule.* The Contractor shall deliver COMSATCOM services in accordance with [552.238-86](#).

(d) *Portability.* The Contractor shall have the capability to redeploy COMSATCOM services, subject to availability. Portability shall be provided within the COMSATCOM Contractor's resources at any time as requested by the ordering activity. When portability is exercised, evidence of equivalent net present value (NPV) shall be provided by the Contractor.

(e) *Flexibility/optimization.* The Contractor shall have the capability to re-groom resources for spectral, operational, or price efficiencies. Flexibility/optimization shall be provided within the COMSATCOM Contractor's resources at any time as requested by the ordering activity. When flexibility/optimization is exercised, evidence of equivalent net present value (NPV) shall be provided by the Contractor. The Contractor is encouraged to submit re-grooming approaches for ordering activity consideration that may increase efficiencies for existing COMSATCOM services.

(f) *Net ready (interoperability).* COMSATCOM services shall be consistent with commercial standards and practices. Services shall have the capability to access and/or interoperate with Government or other Commercial teleports/gateways and provide enterprise service access to or among networks or enclaves. Interfaces may be identified as interoperable on the basis of participation in a sponsored interoperability program.

(g) *Network monitoring (Net OPS)*. The Contractor shall have the capability to electronically collect and deliver near real-time monitoring, fault/incident/outage reporting, and information access to ensure effective and efficient operations, performance, and availability, consistent with commercial practices. Consistent with the Contractor's standard management practices, the Net Ops information will be provided on a frequency (example: every 6 hours, daily) and format (example: SNMP, XML) as defined in a requirement to a location/entity/electronic interface defined by the ordering activity. Specific reporting requirements will be defined by the Ordering Activity.

(h) *EMI/RFI identification, characterization, and geo-location*. The Contractor shall have the capability to collect and electronically report in near real-time Electro Magnetic Interference (EMI) / Radio Frequency Interference (RFI) identification, characterization, and geo-location, including the ability to identify and characterize sub-carrier EMI/RFI being transmitted underneath an authorized carrier, and the ability to geo-locate the source of any and all EMI/RFI. The Contractor shall establish and use with the ordering activity a mutually agreed upon media and voice communications capability capable of protecting "Sensitive, but Unclassified" data.

(i) *Security*. (1) The Contractor may be required to obtain/possess varying levels of personnel and facility security clearances up to U.S. Government TOP SECRET/Sensitive Compartmented Information (TS/SCI) or equivalent clearances assigned by the National Security Authority of a NATO Member State or Major Non-NATO Ally.

(2) For incident resolution involving classified matters, the Contractor shall provide appropriately cleared staff who can affect COMSATCOM services operations (example: satellite payload operations, network operations). The Contractor shall provide a minimum of one operations staff member AND a minimum of one person with the authority to commit the company if resolution requires business impacting decisions (example: Chief Executive Officer, Chief Operations Officer, etc.).

(3) When Communications Security or Transmission Security equipment or keying material is placed in the equipment/terminal shelter, the Contractor shall ensure compliance with applicable physical security directives/guidelines and that all deployed equipment/terminal operations and maintenance personnel shall possess the appropriate clearances, equal to or higher than the classification level of the data being transmitted. Where local regulations require use of foreign personnel for terminal operations and maintenance, then the Contractor shall ensure compliance with applicable security directives/guidelines and document to the U.S. Government's satisfaction that protective measures are in place and such individuals have equivalent clearances granted by the local host nation.

(4) For classified operations security (OPSEC), the Contractor shall ensure that all personnel in direct contact with classified OPSEC indicators (example: the unit, location, and time of operations) have U.S. SECRET or higher personnel security clearances, or, as appropriate, equivalent clearances assigned by the National Security Authority of a NATO Member State or Major Non-NATO Ally, in accordance with applicable security directives and guidelines.

(5) For classified requirements, cleared satellite operator staff must have access to secure voice communications for emergency purposes. Communications security equipment certified by the National Security Agency (NSA) to secure unclassified and up to and including SECRET communication transmissions at all operations centers is preferred. If a Contractor is unable to have access to NSA-approved communications security equipment at its operations centers, then a combination of a "Sensitive but Unclassified" (SBU) cryptographic module approved by the U.S. National Institute for Standards and Technology and pre-arranged access to National Security Agency-approved communications security equipment at an agreed alternate facility is acceptable.

(6) The Contractor shall have the capability to "mask" or "protect" users against unauthorized release of identifying information to any entity that could compromise operations security. Identifying information includes but is not limited to personal user and/or unit information including tail numbers, unit names, unit numbers, individual names, individual contact numbers,

street addresses, etc.

(j) *Third party billing for COMSATCOM subscription services.* The Contractor shall identify authorized network infrastructure for the ordering activity. In some cases, the user of the terminal may access network infrastructure owned or operated by a third party. In the event a terminal is used on a third party's network infrastructure, the Contractor shall provide to the ordering activity, invoices and documentation reflecting actual usage amount and third party charges incurred. The ordering activity shall be billed the actual third party charges incurred, or the contract third party billing price, whichever is less.

**GENERAL SERVICES ADMINISTRATION
Federal Acquisition Service**

AUTHORIZED FEDERAL SUPPLY SCHEDULE FSS PRICE LIST

Online access to contract ordering information, terms and conditions, pricing, and the option to create an electronic delivery order are available through GSA Advantage!®. The website for GSA Advantage!® is: <https://www.GSAAdvantage.gov>.



FSC Group: Information Technology FSC Class: F04

Contract number: 47QTCA24D001Q

Contract period: NOVEMBER 14, 2023 – NOVEMBER 13, 2028

FTR, LTD.
1401 17TH ST, STE525
DENVER, CO 80202
www.fortherecord.com

Contract Administration:
Jeff Hubbs
jhubbs@fortherecord.com
480-980-0380

Business size: Small

For more information on ordering go to the following website: <https://www.gsa.gov/schedules>.

Price list current as of Modification PA-0014 effective 10/30/2024

Prices Shown Herein are Net (discount deducted)

CUSTOMER INFORMATION

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

511210	Software Licenses
54151	Software Maintenance Services
OLM	Order Level Materials

1b. Identification of the lowest priced model number and lowest unit price for that model for each special item number awarded in the contract. This price is the Government price based on a unit of one, exclusive of any quantity/dollar volume, prompt payment, or any other concession affecting price. Those contracts that have unit prices based on the geographic location of the customer, should show the range of the lowest price, and cite the areas to which the prices apply. See Page 4

1c. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles, experience, functional responsibility and education for those types of employees or subcontractors who will perform services shall be provided. If hourly rates are not applicable, indicate "Not applicable" for this item. See Page 4

2. Maximum order: **SINS 511210, 54151, and 33411 - \$500,000**

3. Minimum order: **\$100**

4. Geographic coverage. **Domestic**

5. Point of production. **Same as Company Address**

6. Discount from list prices or statement of net price. **Government Net Prices (discounts already deducted.)**

7. Quantity discounts. **None**

8. Prompt payment terms. Information for Ordering Offices: Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions. **Net 30 days**

9. Foreign items. **Not Applicable**

10a. Time of delivery. **45 days ARO**

10b. Expedited Delivery. Items available for expedited delivery are noted in this price list. **Contact contractor**

10c. Overnight and 2-day delivery. **Contact contractor**

10d. Urgent Requirements. **Contact contractor**

11. F.O.B. point. **Destination**

12a. Ordering address. **Same as Contractors Address**

12b. Ordering procedures: **See Federal Acquisition Regulation (FAR) 8.405-3**

13. Payment address. **Same as Contractors Address**

14. Warranty provision. **FTR warrants that for a period of ninety (90) days from the date of acceptance by ordering agency of For Fee Software, the media on which such For Fee Software was delivered shall be without defects in materials or workmanship. FTR agrees to replace any defective For Fee Software media which is returned to FTR within the foregoing ninety (90) day period.**

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

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

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

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

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

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

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

21. Preventive maintenance (if applicable). **Not Applicable**

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

22b. If applicable, indicate that Section 508 compliance information is available for the information and communications technology (ICT) products and services and show where full details can be found at: <http://community.fortherecord.com/index.php?/files/file/1149-voluntary-product-accessibility-template-gold-56/>
The ICT Accessibility standards can be found at: www.Section508.gov/. **Not applicable**

23. Unique Entity Identifier (UEI) number. **JB Y8FSWTNDM4**

24. Notification regarding registration in System for Award Management (SAM) database. **Contractor registered and active in SAM**

PRICING

MFR PART NO	PRODUCT NAME	PRODUCT DESCRIPTION	UOI	DISCOUNT PRICE OFFERED TO GSA (including IFF)
PWS60699GS10ZN	Premium Support	Premium Support provides In-line version updates (example going from 6.2 to 6.5). Also provides security updates and patches; access to telephone support, and updates to FTR Annotation packages	YR	\$672.85
AUDICUE- SYNC	FTR SYNC Recording Clock	FTR SYNC Recording Clock	EA	\$449.62
PHP02899H Z10ZN	USB/Serial Clock	USB/Serial Clock	EA	\$449.62
FTRGRS7.7	Perpetual Software - FTR Gold Recording Suite 7.7	FTR Gold 7.7 - FTR Gold 7.7 (incl Reporter, Log Notes, Player & Manager)	EA	\$2,792.19
FTRGAS7.7	Perpetual Software - FTR Gold Annotation Suite 7.7	FTR Gold 7.7 Annotation Suite	EA	\$149.62
FTRGRS7.7S	Term Software - FTR Gold Recording Suite 7.7 - Annual Subscription	FTR Gold Recording Suite 7.7 - Software is installed on customer's computer and Term License is for one year - all updates included.	YR	\$1,494.71

Attachment –

Term License Cessation - Term licenses are not eligible for conversion at any time

After a software product has been on a continuous term license for a period of NOT APPLICABLE – This is an annual subscription, a fully paid-up, non-exclusive, perpetual license for the software product shall automatically accrue to the ordering activity. The period of continuous term license for automatic accrual of a fully paid-up perpetual license does not have to be achieved during a particular fiscal year; it is a written Contractor commitment which continues to be available for software that is initially ordered under this contract, until a fully paid-up perpetual license accrues to the ordering activity. However, should the term license of the software be discontinued before the specified period of the continuous term license has been satisfied, the perpetual license accrual shall be forfeited. Contractors who do not commercially offer conversions of term licenses to perpetual licenses shall indicate that their term licenses are not eligible for conversion at any time.

Term licenses are not eligible for conversion at any time

Right-to-Copy Pricing – Not available

Certificate Of Completion

Envelope Id: 11FC3550-3D36-8634-8174-0074FF6BA0FC

Status: Sent

Subject: Council Legislation - For The Record

Source Envelope:

Document Pages: 75

Signatures: 5

Envelope Originator:

Certificate Pages: 16

Initials: 0

Procurement Resource Group

AutoNav: Enabled

730 2nd Ave. South 1st Floor

Envelopeld Stamping: Enabled

Nashville, TN 37219

Time Zone: (UTC-06:00) Central Time (US & Canada)

prg@nashville.gov

IP Address: 170.190.198.185

Record Tracking

Status: Original

Holder: Procurement Resource Group

Location: DocuSign

4/8/2026 10:51:33 AM

prg@nashville.gov

Security Appliance Status: Connected

Pool: StateLocal

Signer Events

Signature

Timestamp

Josh Dhanens

josh.dhanens@nashville.gov

Security Level: Email, Account Authentication
(None)

Sent: 4/8/2026 11:17:03 AM

Viewed: 4/8/2026 11:18:05 AM

Signed: 4/8/2026 11:19:22 AM

Signature Adoption: Pre-selected Style

Using IP Address: 170.190.198.185

Electronic Record and Signature Disclosure:

Not Offered via DocuSign

Dennis Rowland

dennis.rowland@nashville.gov

Purchasing Agent & Chief Procurement Officer

Security Level: Email, Account Authentication
(None)

Sent: 4/8/2026 11:19:34 AM

Viewed: 4/8/2026 6:17:07 PM

Signed: 4/8/2026 6:17:15 PM

Signature Adoption: Pre-selected Style

Using IP Address: 170.190.198.185

Electronic Record and Signature Disclosure:

Not Offered via DocuSign

Jenneen Reed/mjw

MaryJo.Wiggins@nashville.gov

Security Level: Email, Account Authentication
(None)

Sent: 4/8/2026 6:17:24 PM

Viewed: 4/10/2026 10:21:26 AM

Signed: 4/10/2026 10:22:00 AM

Signature Adoption: Pre-selected Style

Using IP Address: 170.190.198.100

Electronic Record and Signature Disclosure:

Accepted: 4/10/2026 10:21:26 AM

ID: 27a65989-e818-4068-84a6-d65f31585a27

Kelli Woodward

Kelli.Woodward@nashville.gov

Security Level: Email, Account Authentication
(None)

Sent: 4/10/2026 10:22:12 AM

Viewed: 4/10/2026 11:36:21 AM

Signed: 4/10/2026 11:36:47 AM

Signature Adoption: Pre-selected Style

Using IP Address: 170.190.198.185

Electronic Record and Signature Disclosure:

Accepted: 4/10/2026 11:36:21 AM

ID: 68348df1-7c38-41cc-8040-c39d72709ea8

Signer Events	Signature	Timestamp
---------------	-----------	-----------

Procurement Resource Group
prg@nashville.gov
Metropolitan Government of Nashville and Davidson
County
Security Level: Email, Account Authentication
(None)
Electronic Record and Signature Disclosure:
Not Offered via DocuSign

In Person Signer Events	Signature	Timestamp
-------------------------	-----------	-----------

Editor Delivery Events	Status	Timestamp
------------------------	--------	-----------

Agent Delivery Events	Status	Timestamp
-----------------------	--------	-----------

Intermediary Delivery Events	Status	Timestamp
------------------------------	--------	-----------

Certified Delivery Events	Status	Timestamp
---------------------------	--------	-----------

Carbon Copy Events	Status	Timestamp
--------------------	--------	-----------

Sally Palmer
sally.palmer@nashville.gov
Security Level: Email, Account Authentication
(None)
Electronic Record and Signature Disclosure:
Accepted: 4/10/2026 10:53:25 AM
ID: 3d504866-5a47-4fdc-92fc-cb106d7b7ef0

Kelli Woodward
Kelli.Woodward@nashville.gov
Security Level: Email, Account Authentication
(None)
Electronic Record and Signature Disclosure:
Accepted: 4/10/2026 11:36:21 AM
ID: 68348df1-7c38-41cc-8040-c39d72709ea8

Amber Gardner
Amber.Gardner@nashville.gov
Security Level: Email, Account Authentication
(None)
Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Austin Kyle
publicrecords@nashville.gov
Security Level: Email, Account Authentication
(None)
Electronic Record and Signature Disclosure:
Accepted: 4/9/2026 12:11:31 PM
ID: 41d5d2be-60da-456d-8297-af5c69db149e

Gary Clay
gary.clay@nashville.gov
Security Level: Email, Account Authentication
(None)
Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Carbon Copy Events	Status	Timestamp
---------------------------	---------------	------------------

John Stewart

john.stewart@nashville.gov

Security Level: Email, Account Authentication
(None)

Electronic Record and Signature Disclosure:

Not Offered via DocuSign

Witness Events	Signature	Timestamp
-----------------------	------------------	------------------

Notary Events	Signature	Timestamp
----------------------	------------------	------------------

Envelope Summary Events	Status	Timestamps
--------------------------------	---------------	-------------------

Envelope Sent

Hashed/Encrypted

4/8/2026 11:17:03 AM

Payment Events	Status	Timestamps
-----------------------	---------------	-------------------

Electronic Record and Signature Disclosure

1. **ACCEPTANCE OF TERMS AND CONDITIONS** These Terms and Conditions govern your ("Subscriber" or "you") use of DocuSign's on-demand electronic signature service (the "Subscription Service"), as accessed either directly through DocuSign.com, DocuSign.net, or through a DocuSign affiliate's™ web page offering a Service Plan (collectively, the "Site"). By depositing any document into the System (as defined below), you accept these Terms and Conditions (including your corresponding Service Plan, the DocuSign.com Terms of Use, and all policies and guidelines referenced and hereby incorporated into these Terms and Conditions) and any modifications that may be made to the Terms and Conditions from time to time. If you do not agree to these Terms and Conditions, you should not use the Subscription Service or visit or browse the Site. These Terms and Conditions constitute a binding legal agreement between you and DocuSign, Inc. ("DocuSign," "we," "us," and "our"). Please read them carefully and print a copy for your future reference.

2. **MODIFICATION OF TERMS AND CONDITIONS** We reserve the right to modify these Terms and Conditions at any time and in any manner at our sole discretion by: (a) posting a revision on the Site; or (b) sending information regarding the amendment to the email address you provide to us. **YOU ARE RESPONSIBLE FOR REGULARLY REVIEWING THE SITE TO OBTAIN TIMELY NOTICE OF ANY AMENDMENTS. YOU SHALL BE DEEMED TO HAVE ACCEPTED SUCH AMENDMENTS BY CONTINUING TO USE THE SUBSCRIPTION SERVICE FOR MORE THAN 20 DAYS AFTER SUCH AMENDMENTS HAVE BEEN POSTED OR INFORMATION REGARDING SUCH AMENDMENTS HAS BEEN SENT TO YOU.** You agree that we shall not be liable to you or to any third party for any modification of the Terms and Conditions.

3. **DEFINITIONS** "Account" means a unique account established by Subscriber to enable its Authorized Users to access and use the Subscription Service. "Authorized User" means any employee or agent of Subscriber, identified by a unique email address and user name, who is registered under the Account, provided that no two persons may register, access or use the Subscription Service as the same Authorized User. "Contract" refers to a contract, notice, disclosure, or other record or document deposited into the System by Subscriber for processing using the Subscription Service. "Envelope" means an electronic record containing one or more eContracts consisting of a single page or a group of pages of data uploaded to the System. "Seat" means an active Authorized User listed in the membership of an Account at any one time. No two individuals may log onto or use the Subscription Service as the same Authorized User, but Subscriber may unregister or deactivate Authorized Users and replace them with other Authorized Users without penalty, so long as the number of active Authorized Users registered at any one time is equal to or less than the number of Seats purchased. "Service Plan" means the right to access and use the Subscription Service for a specified period in exchange for a periodic fee, subject to the Service Plan restrictions and requirements that are used to describe the selected Service Plan on the Site. Restrictions and requirements may include any or all of the following: (a) number of Seats and/or Envelopes that a Subscriber may use in a month or year for a fee; (b) fee for sent Envelopes in excess of the number of Envelopes allocated to Subscriber under the Service Plan; (c) per-seat or per-user restrictions; (d) the license to use DocuSign software products such as DocuSign Connect Express in connection with the Subscription Service; and (e) per use fees. "Specifications" means the technical specifications set forth in the "Subscription Service Specifications" available at <http://docusign.com/company/specifications>. "Subscription Service" means DocuSign's™ on-demand electronic signature service, as updated from time

to time, which provides on-line display, certified delivery, acknowledgement, electronic signature, and storage services for eContracts via the Internet. "System" refers to the software systems and programs, communication and network facilities, and hardware and equipment used by DocuSign or its agents to provide the Subscription Service. "Term" means the period of effectiveness of these Terms and Conditions, as specified in Section 12 below. "Transaction Data" means the metadata associated with an Envelope (such as transaction history, image hash value, method and time of Envelope deletion, sender and recipient names, email addresses and signature IDs) and maintained by DocuSign in order to establish the digital audit trail required by the Subscription Service.

4. SUBSCRIPTION SERVICE

During the term of the Service Plan and subject to these Terms and Conditions, Subscriber will have the right to obtain an Account and register its Authorized Users, who may access and use the Subscription Service, and DocuSign will provide the Subscription Service in material conformance with the Specifications. You must be 18 years of age or older to register for an Account and use the Subscription Service. Subscriber's right to use the Subscription Service is limited to its Authorized Users, and Subscriber agrees not to resell or otherwise provide or assist with the provision of the Subscription Service to any third party. In addition, DocuSign's provision of the Subscription Service is conditioned on Subscriber's acknowledgement and agreement to the following: (a) The Subscription Service facilitates the execution of eContracts between the parties to those eContracts. Nothing in these Terms and Conditions may be construed to make DocuSign a party to any eContract processed through the Subscription Service, and DocuSign makes no representation or warranty regarding the transactions sought to be effected by any eContract; (b) Between DocuSign and Subscriber, Subscriber has exclusive control over and responsibility for the content, quality, and format of any eContract. All eContracts stored by DocuSign are maintained in an encrypted form, and DocuSign has no control of or access to their contents; (c) If Subscriber elects to use one or more of the optional features designed to verify the identity of the intended recipient of an eContract that DocuSign makes available to its subscribers ("Authentication Measures"), DocuSign will apply only those Authentication Measures selected by the Subscriber, but makes no representations or warranties about the appropriateness of any Authentication Measure. Further, DocuSign assumes no liability for: (A) the inability or failure by the intended recipient or other party to satisfy the Authentication Measure; or (B) the circumvention by any person (other than DocuSign) of any Authentication Measure; (d) Certain types of agreements and documents may be exempted from electronic signature laws (e.g. wills and agreements pertaining to family law), or may be subject to specific regulations promulgated by various government agencies regarding electronic signatures and electronic records. DocuSign is not responsible or liable to determine whether any particular eContract is subject to an exception to applicable electronic signature laws, or whether it is subject to any particular agency promulgations, or whether it can be legally formed by electronic signatures; (e) DocuSign is not responsible for determining how long any d to be retained or stored under any applicable laws, regulations, or legal or administrative agency processes. Further, DocuSign is not responsible for or liable to produce any of Subscriber's eContracts or other documents to any third parties; (f) Certain consumer protection or similar laws or regulations may impose special requirements with respect to electronic transactions involving one or more "consumers," such as (among others) requirements that the consumer consent to the method of contracting and/or that the consumer be provided with a copy, or access to a copy, of a paper or other non-electronic, written record of the transaction. DocuSign does not and is not responsible to: (A) determine whether any

particular transaction involves a “consumer”; (B) furnish or obtain any such consents or determine if any such consents have been withdrawn; (C) provide any information or disclosures in connection with any attempt to obtain any such consents; (D) provide legal review of, or update or correct any information or disclosures currently or previously given; (E) provide any such copies or access, except as expressly provided in the Specifications for all transactions, consumer or otherwise; or (F) otherwise to comply with any such special requirements; and (g) Subscriber undertakes to determine whether any “consumer” is involved in any eContract presented by Subscriber or its Authorized Users for processing, and, if so, to comply with all requirements imposed by law on such eContracts or their formation. (h) If the domain of the primary email address associated with the Account is owned by an organization and was assigned to Subscriber as an employee, contractor or member of such organization, and that organization wishes to establish a commercial relationship with DocuSign and add the Account to such relationship, then, if Subscriber does not change the email address associated with the Account, the Account may become subject to the commercial relationship between DocuSign and such organization and controlled by such organization.

5. RESPONSIBILITY FOR CONTENT OF COMMUNICATIONS As between Subscriber and DocuSign, Subscriber is solely responsible for the nature and content of all materials, works, data, statements, and other visual, graphical, video, and written or audible communications submitted by any Authorized User or otherwise processed through its Account, the Subscription Service, or under any Service Plan. Accordingly: (a) Subscriber will not use or permit the use of the Subscription Service to send unsolicited mass mailings outside its organization. The term “unsolicited mass mailings” includes all statutory or common definitions or understanding of those terms in the applicable jurisdiction, such as those set forth for “Commercial Electronic Mail Messages” under the U.S. CAN-SPAM Act, as an example only; and (b) Subscriber will not use or permit the use of the Subscription Service: (i) to communicate any message or material that is defamatory, harassing, libelous, threatening, or obscene; (ii) in a way that violates or infringes upon the intellectual property rights or the privacy or publicity rights of any person or entity or that may otherwise be unlawful or give rise to civil or criminal liability (other than contractual liability of the parties under eContracts processed through the Subscription Service); (iii) in any manner that is likely to damage, disable, overburden, or impair the System or the Subscription Service or interfere with the use or enjoyment of the Subscription Service by others; or (iv) in any way that constitutes or encourages conduct that could constitute a criminal offense. DocuSign does not monitor the content processed through the Subscription Service, but in accordance with DMCA (Digital Millennium Copyright Act) safe harbors, it may suspend any use of the Subscription Service, or remove or disable any content that DocuSign reasonably and in good faith believes violates this Agreement or applicable laws or regulations. DocuSign will use commercially reasonable efforts to notify Subscriber prior to any such suspension or disablement, unless DocuSign reasonably believes that: (A) it is prohibited from doing so under applicable law or under legal process, such as court or government administrative agency processes, orders, mandates, and the like; or (B) it is necessary to delay notice in order to prevent imminent harm to the System, Subscription Service, or a third party. Under circumstances where notice is delayed, DocuSign will provide the notice if and when the related restrictions in the previous sentence no longer apply.

6. PRICING AND PER USE PURCHASES The prices, features, and options of the Subscription Service available for an Account depend on the Service Plan selected by Subscriber. Subscriber may also purchase optional services on a periodic or per-use basis. DocuSign may add or change the prices, features or options available with a

Service Plan without notice. Subscriber's usage under a Service Plan is measured based on the actual number of Seats as described in the Service Plan on the Site. Once a per-Seat Service Plan is established, the right of the named Authorized User to access and use the Subscription Service is not transferable; any additional or differently named Authorized Users must purchase per-Seat Service Plans to send Envelopes. Extra seats, users and/or per use fees will be charged as set forth in Subscriber's Service Plan if allowed by such Service Plan. If a Services Plan defines a monthly Envelope Allowance (i.e. # Envelopes per month allowed to be sent), all Envelopes sent in excess of the Envelope Allowance will incur a per-Envelope charge. Any unused Envelope Allowances will expire and not carry over from one billing period to another under a Service Plan. Subscriber's Account will be deemed to have consumed an Envelope at the time the Envelope is sent by Subscriber, regardless of whether Envelopes were received by recipients, or whether recipients have performed any actions upon any eContract in the Envelope. Powerforms are considered Envelopes within an Envelope Allowance Service Plan, and will be deemed consumed at the time they are "clicked" by any end user regardless of whether or not any actions are subsequently performed upon such Envelope. For Service Plans that specify the Envelope Allowance is "Unlimited," Subscriber is allowed to send a reasonable number of Envelopes from the number of Seats purchased. If DocuSign suspects that the number of Envelopes sent from a particular Seat or a group of Seats is abusive and/or unduly burdensome, DocuSign will promptly notify Subscriber, discuss the use-case scenario with Subscriber and any continued monitoring, additional discussions and/or information required to make a final determination on the course of action based on such information. In the event Subscriber exceeds, in DocuSign's sole discretion, reasonable use restrictions under a Service Plan, DocuSign reserves the right to transfer Subscriber into a higher-tier Service Plan without notice. If you misrepresent your eligibility for any Service Plan, you agree to pay us the additional amount you would have been charged under the most favorable pricing structure for which you are eligible. DocuSign may discontinue a Service Plan at any time, and with prior notice to you, may migrate your Account to a similar Service Plan that may carry a different fee. You agree to allow us to charge your credit card for the fees associated with a substitute Service Plan, even if those fees are higher than those you agreed to when you registered your Account. Optional asures, are measured at the time of use, and such charges are specific to the number of units of the service(s) used during the billing period. Optional services subject to periodic charges, such as additional secure storage, are charged on the same periodic basis as the Service Plan fees for the Subscription Service.

7. SUBSCRIBER SUPPORT DocuSign will provide Subscriber support to Subscriber as specified in the Service Plan selected by Subscriber, and that is further detailed on DocuSign's website.

8. STORAGE DocuSign will store eContracts per the terms of the Service Plan selected by Subscriber. For Service Plans that specify the Envelope storage amount is "Unlimited," DocuSign will store an amount of Envelopes that is not abusive and/or unduly burdensome, in DocuSign's sole discretion. Subscriber may retrieve and store copies of eContracts for storage outside of the System at any time during the Term of the Service Plan when Subscriber is in good financial standing under these Terms and Conditions, and may delete or purge eContracts from the System at its own discretion. DocuSign may, at its sole discretion, delete an uncompleted eContract from the System immediately and without notice upon earlier of: (i) expiration of the Envelope (where Subscriber has established an expiration for such Envelope, not to exceed 365 days); or (ii) expiration of the Term. DocuSign assumes no liability or responsibility for a party's failure or inability to electronically sign any eContract within such a period of time. DocuSign may retain Transaction Data for as long as it has a

business purpose to do so. 9. BUSINESS AGREEMENT BENEFITS You may receive or be eligible for certain pricing structures, discounts, features, promotions, and other benefits (collectively, "Benefits") through a business or government Subscriber's agreement with us (a "Business Agreement"). Any and all such Benefits are provided to you solely as a result of the corresponding Business Agreement and such Benefits may be modified or terminated without notice. If you use the Subscription Service where a business or government entity pays your charges or is otherwise liable for the charges, you authorize us to share your account information with that entity and/or its authorized agents. If you are enrolled in a Service Plan or receive certain Benefits tied to a Business Agreement with us, but you are liable for your own charges, then you authorize us to share enough account information with that entity and its authorized agents to verify your continuing eligibility for those Benefits and the Service Plan. 10. FEES AND PAYMENT TERMS The Service Plan rates, charges, and other conditions for use are set forth in the Site. Subscriber will pay DocuSign the applicable charges for the Services Plan as set forth on the Site. If you add more Authorized Users than the number of Seats you purchased, we will add those Authorized Users to your Account and impose additional charges for such additional Seats on an ongoing basis. Charges for pre-paid Service Plans will be billed to Subscriber in advance. Charges for per use purchases and standard Service Plan charges will be billed in arrears. When you register for an Account, you will be required to provide DocuSign with accurate, complete, and current credit card information for a valid credit card that you are authorized to use. You must promptly notify us of any change in your invoicing address or changes related to the credit card used for payment. By completing your registration for the Services Plan, you authorize DocuSign or its agent to bill your credit card the applicable Service Plan charges, any and all applicable taxes, and any other charges you may incur in connection with your use of the Subscription Service, all of which will be charged to your credit card. Each time you use the Subscription Service, or allow or cause the Subscription Service to be used, you reaffirm that we are authorized to charge your credit card. You may terminate your Account and revoke your credit card authorization as set forth in the Term and Termination section of these Terms and Conditions. We will provide you with one invoice in a format we choose, which may change from time to time, for all Subscription Service associated with each Account and any charges of a third party on whose behalf we bill. Payment of all charges is due and will be charged to your credit card upon your receipt of an invoice. Billing cycle end dates may change from time to time. When a billing cycle covers less than or more than a full month, we may make reasonable adjustments and/or prorations. If your Account is a qualified business account and is approved by us in writing for corporate billing, charges will be accumulated, identified by Account identification number, and invoiced on a monthly basis. You agree that we may (at our option) accumulate charges incurred during your monthly billing cycle and submit them as one or more aggregate charges during or at the end of each cycle, and that we may delay obtaining authorization from your credit card issuer until submission of the accumulated charge(s). This means that accumulated charges may appear on the statement you receive from your credit card issuer. If DocuSign does not receive payment from your credit card provider, you agree to pay all amounts due upon demand. DocuSign reserves the right to correct any errors or mistakes that it makes even if it has already requested or received payment. Your credit card issuer's agreement governs your use of your credit card in connection with the Subscription Service, and you must refer to such agreement (not these Terms and Conditions) with respect to your rights and liabilities as a cardholder. You are solely responsible for any and all fees charged to your credit card by the issuer, bank, or financial institution including, but not limited to, membership,

overdraft, insufficient funds, and over the credit limit fees. You agree to notify us about any billing problems or discrepancies within 20 days after they first appear on your invoice. If you do not bring them to our attention within 20 days, you agree that you waive your right to dispute such problems or discrepancies. We may modify the price, content, or nature of the Subscription Service and/or your Service Plan at any time. If we modify any of the foregoing terms, you may cancel your use of the Subscription Service. We may provide notice of any such changes by e-mail, notice to you upon log-in, or by publishing them on the Site. Your payment obligations survive any termination of your use of the Subscription Service before the end of the billing cycle. Any amount not paid when due will be subject to finance charges equal to 1.5% of the unpaid balance per month or the highest rate permitted by applicable usury law, whichever is less, determined and compounded daily from the date due until the date paid. Subscriber will reimburse any costs or expenses (including, but not limited to, reasonable attorneys' fees) incurred by DocuSign to collect any amount that is not paid when due. DocuSign may accept any check or payment in any amount without prejudice to DocuSign's right to recover the balance of the amount due or to pursue any other right or remedy. Amounts due to DocuSign under these Terms and Conditions may not be withheld or offset by Subscriber for any reason against amounts due or asserted to be due to Subscriber from DocuSign. Unless otherwise noted and Conditions are denominated in United States dollars, and Subscriber will pay all such amounts in United States dollars. Other than federal and state net income taxes imposed on DocuSign by the United States, Subscriber will bear all taxes, duties, VAT and other governmental charges (collectively, "taxes") resulting from these Terms and Conditions or transactions conducted in relation to these Terms and Conditions. Subscriber will pay any additional taxes as are necessary to ensure that the net amounts received and retained by DocuSign after all such taxes are paid are equal to the amounts that DocuSign would have been entitled to in accordance with these Terms and Conditions as if the taxes did not exist. 11. DEPOSITS, SERVICE LIMITS, CREDIT REPORTS, AND RETURN OF BALANCES You authorize us to ask consumer reporting agencies or trade references to furnish us with employment and credit information, and you consent to our rechecking and reporting personal and/or business payment and credit history if, in our sole discretion, we so choose. If you believe that we have reported inaccurate information about your account to a consumer reporting agency, you may send a written notice describing the specific inaccuracy to the address provided in the Notices section below. For you to use the Subscription Service, we may require a deposit or set a service limit. The deposit will be held as a partial guarantee of payment. It cannot be used by you to pay your invoice or delayed payment. Unless otherwise required by law, deposits may be mixed with other funds and will not earn interest. We reserve the right to increase your deposit if we deem appropriate. You may request that we reevaluate your deposit on an annual basis, which may result in a partial or total refund of the deposit to you or credit to your account. If you default or these Terms and Conditions are terminated, we may, without notice to you, apply any deposit towards payment of any amounts you owe to us. After approximately 90 days following termination of these Terms and Conditions, any remaining deposit or other credit balance in excess of amounts owed will be returned without interest, unless otherwise required by law, to you at your last known address. You agree that any amounts under \$15 will not be refunded to cover our costs of closing your account. If the deposit balance is undeliverable and returned to us, we will hold it for you for one year from the date of return and, during that period, we may charge a service fee against the deposit balance. You hereby grant us a security interest in any deposit we require to secure the performance of your obligations under these Terms and

Conditions. 12. TERM AND TERMINATION The term of these Terms and Conditions for each Account begins on the date you register for an Account and continues for the term specified by the Service Plan you purchase (the "Term"). You may terminate your Account at any time upon 10 days advance written notice to DocuSign following the Notice procedures set forth in these Terms and Conditions. Unless you terminate your Account or you set your Account to not auto renew, your Service Plan will automatically renew at the end of its Term (each a "Renewal Term"), and you authorize us (without notice) to collect the then-applicable fee and any taxes for the renewed Service Plan, using any credit card we have on record for you. Service Plan fees and features may change over time. Your Service Plan for a Renewal Term will be the one we choose as being closest to your Service Plan from the prior Term. For any termination (including when you switch your Account), you will be responsible for payment of all fees and charges through the end of the billing cycle in which termination occurs. If you terminate your annual Service Plan Account within the first 30 days of the Term, you may submit written request to DocuSign following the Notice procedures set forth in these Terms and Conditions, for a full refund of the prepaid fees paid by you to DocuSign. You will be limited to one refund. You agree that termination of an annual Service Plan after the first 30 days will not entitle you to any refund of prepaid fees. You will be in default of these Terms and Conditions if you: (a) fail to pay any amount owed to us or an affiliate of ours or any amount appearing on your invoice; (b) have amounts still owing to us or an affiliate of ours from a prior account; (c) breach any provision of these Terms and Conditions; (d) violate any policy applicable to the Subscription Service; (e) are subject to any proceeding under the Bankruptcy Code or similar laws; or (f) if, in our sole discretion, we believe that your continued use of the Subscription Service presents a threat to the security of other users of the Subscription Service. If you are in default, we may, without notice to you, suspend your Account and use of the Subscription Service, withhold refunds and terminate your Account, in addition to all other remedies available to us. We may require reactivation charges to reactivate your Account after termination or suspension. The following provisions will survive the termination of these Terms and Conditions and your Account: Sections 3, 9-11, and 15-23. 13. SUBSCRIBER WARRANTIES You hereby represent and warrant to DocuSign that: (a) you have all requisite rights and authority to use the Subscription Service under these Terms and Conditions and to grant all applicable rights herein; (b) the performance of your obligations under these Terms and Conditions will not violate, conflict with, or result in a default under any other agreement, including confidentiality agreements between you and third parties; (c) you will use the Subscription Service for lawful purposes only and subject to these Terms and Conditions; (d) you are responsible for all use of the Subscription Service in your Account; (e) you are solely responsible for maintaining the confidentiality of your Account names and password(s); (f) you agree to immediately notify us of any unauthorized use of your Account of which you become aware; (g) you agree that DocuSign will not be liable for any losses incurred as a result of a third party's use of your Account, regardless of whether such use is with or without your knowledge and consent; (h) you will not use the Subscription Service in any manner that could damage, disable, overburden or impair the System, or interfere with another's use of the Subscription Service by others; (i) any information submitted to DocuSign by you is true, accurate, and correct; and (j) you will not attempt to gain unauthorized access to the System or the Subscription Service, other accounts, computer systems, or networks under the control or responsibility of DocuSign through hacking, cracking, password mining, or any other unauthorized means. 14. DOCUSIGN WARRANTIES DocuSign represents and warrants that: (a) the Subscription Service as delivered to Subscriber

and used in accordance with the Specifications will not infringe on any United States patent, copyright or trade secret; (b) the Subscription Service will be performed in accordance with the Specifications in their then-current form at the time of the provision of such Subscription Service; (c) any DocuSign Products that are software shall be free of harmful or illicit code, trapdoors, viruses, or other harmful features; (d) the proper use of the Subscription Service by Subscriber in accordance with the Specifications and applicable law in the formation of an eContract not involving any consumer will be sufficient under the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. Â§Â§ 7001 et seq. (the "ESIGN Act") to ESIGN Act; (e) the proper use of the Subscription Service by Subscriber in accordance with the Specifications and applicable law in the formation of an eContract involving a consumer will be sufficient under the ESIGN Act to support the validity of such formation, to the extent provided in the ESIGN Act, so long as and provided that Subscriber complies with all special requirements for consumer eContracts, including and subject to those referenced in Section 4.(f) and (g) above; and (f) DocuSign has implemented information security policies and safeguards to preserve the security, integrity, and confidentiality of eContracts and to protect against unauthorized access and anticipated threats or hazards thereto, that meet the objectives of the Interagency Guidelines Establishing Standards for Safeguarding Subscriber Information as set forth in Section 501 (b) of the Gramm-Leach-Bliley Act.

15. DISCLAIMER OF WARRANTIES EXCEPT FOR THE REPRESENTATIONS AND WARRANTIES EXPRESSLY PROVIDED IN SECTION 14 OF THESE TERMS AND CONDITIONS, THE SUBSCRIPTION SERVICE AND THE SITE ARE PROVIDED "AS IS," AND DOCUSIGN: (a) MAKES NO ADDITIONAL REPRESENTATION OR WARRANTY OF ANY KIND WHETHER EXPRESS, IMPLIED (EITHER IN FACT OR BY OPERATION OF LAW), OR STATUTORY, AS TO ANY MATTER WHATSOEVER; (b) EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, QUALITY, ACCURACY, AND TITLE; AND (c) DOES NOT WARRANT THAT THE SUBSCRIPTION SERVICE OR SITE ARE OR WILL BE ERROR-FREE, WILL MEET SUBSCRIBER'S REQUIREMENTS, OR BE TIMELY OR SECURE. SUBSCRIBER WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE RESULTING FROM THE USE OF THE SUBSCRIPTION SERVICE OR SITE. SUBSCRIBER WILL NOT HAVE THE RIGHT TO MAKE OR PASS ON ANY REPRESENTATION OR WARRANTY ON BEHALF OF DOCUSIGN TO ANY THIRD PARTY. USE OF THE SUBSCRIPTION SERVICE AND SITE ARE AT YOUR SOLE RISK. Because some states and jurisdictions do not allow limitations on implied warranties, the above limitation may not apply to you. In that event, such warranties are limited to the minimum warranty period allowed by the applicable law.

16. SUBSCRIBER INDEMNIFICATION OBLIGATIONS You will defend, indemnify, and hold us, our affiliates, officers, directors, employees, suppliers, consultants, and agents harmless from any and all third party claims, liability, damages, and costs (including, but not limited to, attorneys' fees) arising from or related to: (a) your use of the Subscription Service; (b) your violation of these Terms and Conditions; (c) your infringement, or infringement by any other user of your Account, of any intellectual property or other right of any person or entity; or (d) the nature and content of all materials, works, data, statements, and other visual, graphical, written, or audible communications of any nature submitted by any Authorized User of your Account or otherwise processed through your Account.

17. LIMITATIONS OF LIABILITY NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED IN THESE TERMS AND CONDITIONS, DOCUSIGN WILL NOT, UNDER ANY CIRCUMSTANCES, BE LIABLE TO SUBSCRIBER

FOR ANY CONSEQUENTIAL, INCIDENTAL, SPECIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR RELATED TO THE TRANSACTIONS CONTEMPLATED UNDER THESE TERMS AND CONDITIONS, INCLUDING BUT NOT LIMITED TO LOST PROFITS OR LOSS OF BUSINESS, EVEN IF APPRISED OF THE LIKELIHOOD OF SUCH DAMAGES OCCURRING. UNDER NO CIRCUMSTANCES WILL DOCUSIGN'S TOTAL LIABILITY OF ALL KINDS ARISING OUT OF OR RELATED TO THESE TERMS AND CONDITIONS OR SUBSCRIBER'S USE OF THE SUBSCRIPTION SERVICE (INCLUDING BUT NOT LIMITED TO WARRANTY CLAIMS), REGARDLESS OF THE FORUM AND REGARDLESS OF WHETHER ANY ACTION OR CLAIM IS BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, EXCEED THE TOTAL AMOUNT PAID BY SUBSCRIBER TO DOCUSIGN UNDER THESE TERMS AND CONDITIONS DURING THE 3 MONTHS PRECEDING THE DATE OF THE ACTION OR CLAIM. EACH PROVISION OF THESE TERMS AND CONDITIONS THAT PROVIDES FOR A LIMITATION OF LIABILITY, DISCLAIMER OF WARRANTIES, OR EXCLUSION OF DAMAGES REPRESENTS AN AGREED ALLOCATION OF THE RISKS OF THESE TERMS AND CONDITIONS BETWEEN THE PARTIES. THIS ALLOCATION IS REFLECTED IN THE PRICING OFFERED BY DOCUSIGN TO SUBSCRIBER AND IS AN ESSENTIAL ELEMENT OF THE BASIS OF THE BARGAIN BETWEEN THE PARTIES. EACH OF THESE PROVISIONS IS SEVERABLE AND INDEPENDENT OF ALL OTHER PROVISIONS OF THESE TERMS AND CONDITIONS, AND EACH OF THESE PROVISIONS WILL APPLY EVEN IF THE WARRANTIES IN THESE TERMS AND CONDITIONS HAVE FAILED OF THEIR ESSENTIAL PURPOSE. Because some states and jurisdictions do not allow limitation of liability in certain instances, portions of the above limitation may not apply to you.

18. CONFIDENTIALITY – "Confidential Information" means any trade secrets or other information of DocuSign, whether of a technical, business, or other nature (including, without limitation, DocuSign software and related information), that is disclosed to or made available to Subscriber. Confidential Information does not include any information that: (a) was known to Subscriber prior to receiving it from DocuSign; (b) is independently developed by Subscriber without use of or reference to any Confidential Information; (c) is acquired by Subscriber from another source without restriction as to use or disclosure; or (d) is or becomes part of the public domain through no fault or action of Subscriber. During and after the Term of these Terms and Conditions, Subscriber will: (i) use the Confidential Information solely for the purpose for which it is provided; (ii) not disclose such Confidential Information to a third party; and (iii) protect such Confidential Information from unauthorized use and disclosure to the same extent (but using no less than a reasonable degree of care) that it protects its own Confidential Information of a similar nature. If Subscriber is required by law to disclose the Confidential Information or the terms of these Terms and Conditions, Subscriber must give prompt written notice of such requirement before such disclosure and assist the DocuSign in obtaining an order protecting the Confidential Information from public disclosure. Subscriber acknowledges that, as between the parties, all Confidential Information it receives from DocuSign, including all copies thereof in Subscriber's possession or control, in any media, is proprietary to and exclusively owned by DocuSign. Nothing in these Terms and Conditions grants Subscriber any right, title, or interest in or to any of the Confidential Information. Subscriber's incorporation of the Confidential Information into any of its own materials shall not render Confidential Information non-confidential. Subscriber acknowledges that any actual or threatened violation of this confidentiality provision may cause

irreparable, non-monetary injury to the disclosing party, the extent of which may be difficult to ascertain, and therefore agrees that DocuSign shall be entitled to seek injunctive relief in addition to all remedies available to DocuSign at law and/or in equity. Absent written consent of DocuSign, the burden of proving that the Confidential Information is not, or is no longer, confidential or a trade secret shall be on Subscriber.

19. **PRIVACY** Personal information provided or collected through or in connection with this Site shall only be used in accordance with DocuSign's Privacy Policy and these Terms and Conditions are subject to the Privacy Policy on DocuSign's website which sets forth the terms and conditions governing DocuSign's collection and use of personal information from Authorized Users that is gathered through the Site.

20. **ACCESS LIMITS** Your use of the Site is at all times governed by our website Terms of Service. DocuSign is the owner of various intellectual property and technology rights associated with the Subscription Service, its document management, digital signature, and notary system, including patent, copyright, trade secret, and trademark and service mark rights. Except for the rights expressly granted in these Terms and Conditions, DocuSign does not transfer to Subscriber of any Authorized User any of DocuSign's technology or other intellectual property or technology rights. All right, title, and interest in and to DocuSign's technology and intellectual property will remain solely with the DocuSign. Subscriber agrees that it will not, directly or indirectly, reverse engineer, decompile, disassemble, or otherwise attempt to derive source code or other trade secrets from the Subscription Service or DocuSign's technology. DocuSign agrees that data and information provided by Subscriber under these Terms and Conditions shall remain, as between Subscriber and DocuSign, owned by Subscriber. DocuSign hereby grants to users and licensees of its products and services a limited, revocable, nonexclusive and nontransferable right to use DocuSign's regular trade names, trademarks, titles and logos ("Licensed Marks") solely for purposes of identifying DocuSign's products and services. Details of this trademark license are available at: <http://www.docusign.com/IP>.

22. **FEEDBACK** By submitting feedback to DocuSign: (a) Subscriber automatically grants to DocuSign a perpetual, irrevocable, transferable, royalty-free license to use Subscriber's feedback for any and all purposes without any compensation to Subscriber; and (b) Subscriber agrees that it will not publish, submit, or display feedback submitted by Subscriber or its Authorized Users to or on any other web site or in any other publicly accessible forum without DocuSign's prior written consent.

23. **GENERAL** Subscriber acknowledges that the Subscription Service and any related products, information, documentation, software, technology, technical data, and any derivatives thereof, that DocuSign makes available to its Subscribers (collectively "Excluded Data"), is subject to export control laws and regulations of the United States and other jurisdictions (collectively "Export Laws"). Subscriber represents and warrants that: (i) it is not located in, under the control of, or a national or resident of an embargoed country or prohibited end user under Export Laws; and (ii) it will not access, download, use, export or re-export, directly or indirectly, the Excluded Data to any location, entity, government or person prohibited by export laws, without first complying with all Export Laws that may be imposed by the U.S. Government and any country or organization of nations within whose jurisdiction it operates or does business. Subscriber is solely responsible for complying with Export Laws for all Excluded Data and any of its content transmitted through the Subscription Service. Subscriber shall advise DocuSign in the event the Excluded Data requires DocuSign to obtain additional licenses, permits and/or approvals from any government in the jurisdiction where Subscriber intends to use the Subscription Service. Upon being advised of such a requirement, DocuSign may at its sole discretion: (a) terminate

Subscriber's Account; (b) obtain such licenses, permits, and/or approvals as may be required; or (c) modify these Terms and Conditions such that additional licenses, permits, and/or approvals are no longer required to be obtained by DocuSign. The Subscription Service will be accessed and delivered via the internet. Subscriber is responsible for obtaining the necessary equipment and internet connection in order to access and use the Subscription Service. In order to fully utilize the Subscription Service, Subscriber will need to maintain certain minimum hardware and software requirements. These requirements are set forth in the Specifications. DocuSign will be and act as an independent contractor (and not as the agent or representative of Subscriber) in the performance of these Terms and Conditions. These Terms and Conditions will not be interpreted or construed as: (a) creating or evidencing any association, joint venture, partnership, or franchise between the parties; (b) imposing any partnership or franchise obligation or liability on either party; (c) prohibiting or restricting either party's performance of any services for any third party; or (d) establishing or as a foundation for any rights or remedies for any third party, whether as a third party beneficiary or otherwise. Subscriber must not represent to anyone that Subscriber is an agent of DocuSign or is otherwise authorized to bind or commit DocuSign in any way without DocuSign's prior authorization. Subscriber may not assign its rights, duties, or obligations under these Terms and Conditions without DocuSign's prior written consent. If consent is given, these Terms and Conditions will bind Subscriber's successors and assigns. Any attempt by Subscriber to transfer its rights, duties, or obligations under these Terms and Conditions except as expressly provided in these Terms and Conditions is void. DocuSign may freely assign its rights, duties, and obligations under these Terms and Conditions. DocuSign may utilize a subcontractor or other third party to perform its duties under these Terms and Conditions so long as: (a) DocuSign shall not be relieved of any responsibilities or obligations under these Terms and Conditions that are performed by the subcontractor or third party; and (b) DocuSign shall remain Subscriber's sole point of contact and sole contracting party. We may provide, or third parties may provide, links to other Web sites or resources that are beyond our control. We make no representations as to the quality, suitability, functionality, or legality of any sites to which links may be provided, and you hereby waive any claim you might have against us with respect to such sites. **DOCUSIGN IS NOT RESPONSIBLE FOR THE CONTENT ON THE INTERNET OR WEB PAGES THAT ARE CONTAINED OUTSIDE THE SITE.** Your correspondence or business dealings with, or participation in promotions of, advertisers or partners found on or through the Site, including payment and delivery of related goods or services, and any other terms, conditions, warranties, or representations associated with such dealings, are solely between you and such advertiser or partner. You agree that we are not responsible or liable for any loss or damage of any sort incurred as the result of any such dealings or as the result of the presence of such advertisers or partners on the Site. Any notice required or permitted to be given in accordance with these Terms and Conditions will be effective if it is in writing and sent using the certified delivery function of the Subscription Service, by email, certified or registered mail, or insured courier, return receipt requested, to the appropriate party at the address set forth in Subscriber's registration information for Subscriber or on the Site for DocuSign. Either party may change its address for receipt of notice by notice to the other party in accordance with this Section. Notices are deemed given upon receipt if delivered using the Subscription Service or email, two business days following the date of mailing, or one business day following delivery to a courier. Written notification to terminate an Account shall be sent by email to support@docuSign.com from the Subscriber's email address set forth in Subscriber's registration information for Subscriber, or by calling

1.866.219.4318. Neither party will be liable for, or be considered to be in breach of or default on account of, any delay or failure to perform as required by these Terms and Conditions as a result of any cause or condition beyond such party's reasonable control, so long as such party uses all commercially reasonable efforts to avoid or remove such causes of non-performance or delay. These Terms and Conditions are governed in all respects by the laws of the State of Washington as such laws are applied to agreements entered into and to be performed entirely within Washington between Washington residents. Any controversy or claim arising out of or relating to these Terms and Conditions, the Hosted Service, or the Site will be settled by binding arbitration in accordance with the commercial arbitration rules of the American Arbitration Association. Any such controversy or claim shall be arbitrated on an individual basis, and shall not be consolidated in any arbitration with any claim or controversy of any other party. The arbitration will be conducted in King County, Washington, and judgment on the arbitration award may be entered into any court having jurisdiction thereof. The award of the arbitrator shall be final and binding upon the parties without appeal or review except as permitted by Washington law. Notwithstanding the foregoing, either party may seek any interim or preliminary injunctive relief from any court of competent jurisdiction, as necessary to protect the party's rights or property pending the completion of arbitration. By using the Site or the Subscription Service, you consent and submit to the exclusive jurisdiction and venue of the state and federal courts located in King County, Washington. Any legal action by Subscriber arising under these Terms and Conditions must be initiated within two years after the cause of action arises. The waiver by either party of any breach of any provision of these Terms and Conditions does not waive any other breach. The failure of any party to insist on strict performance of any covenant or obligation in accordance with these Terms and Conditions will not be a waiver of such party's right to demand strict compliance in the future, nor will the same be construed as a novation of these Terms and Conditions. If any part of these Terms and Conditions is found to be illegal, unenforceable, or invalid, the remaining portions of these Terms and Conditions will remain in full force and effect. If any material limitation or restriction on the grant of any license to Subscriber under these Terms and Conditions is found to be illegal, unenforceable, or invalid, the license will immediately terminate. Except as set forth in Section 2 of these Terms and Conditions, these Terms and Conditions may not be amended except in writing signed by both you and us. In the event that we make such a change that has a material adverse impact on your rights or use of the Service, you may terminate these Terms and Conditions by giving us notice within 20 days of the date we notify you, and you will not be charged any cancellation fee. These Terms and Conditions are the final and complete expression of the agreement between these parties regarding the Subscription Service. These Terms and Conditions supersede, and the terms of these Terms and Conditions govern, all previous oral and written communications regarding these matters.

v140527 How it works eSignature Digital Transaction Management Legality Security Global Take a Demo Free Trial Resource Center By Industry Financial Services Healthcare High Tech Higher Education Insurance Real Estate Life Sciences Government By Department Sales Human Resources Finance IT/Operations Legal Marketing Facilities Support Product Management Procurement Partners & Developers Partner Programs Find a Partner Solution Showcase Partner Portal Dev Center Support & Training DocuSign Support Community DocuSign University Company About DocuSign Leadership Team Financial Investors Board of Directors Security & Trust Blog Events Press Room Careers Contact Subscriptions Follow Us Facebook Twitter LinkedIn Glassdoor Google + YouTube Validate TRUSTe privacy certification © DocuSign Inc., 2003 - 2014 221 Main St., Suite 1000, San

Francisco, CA 94105 Sales: +1.877.720.2040 | Support: +1.866.219.4318 North America Terms of Use Privacy Policy Intellectual Property Trending Topics: Digital Signature Free What Is Electronic Signature Pdf App For Signing Documents Sign Documents On Android What Is Digital Signature Processing DocuSign FREE TRIAL BUY NOW Validate TRUSTe privacy certification .