Combined Solicitation Refresh
for
ICAM, Mobility, and HACS SIN Rewrites

----- Beginning Regulation -----

SCP-FSS-004 SPECIFIC PROPOSAL INSTRUCTIONS FOR SCHEDULE 70 (AUG 2017)

(a) Read the entire solicitation document prior to preparation of an offer.

(b) CRITICAL INFORMATION - See attachment "Critical Information Specific to Schedule 70." Thoroughly read the attachment for additional information, requirements, and terms and conditions specific to Schedule 70.

(c) The Offeror must comply with the instructions outlined in either SCP-FSS-001-N *Instructions Applicable to New Offerors (Alternate I – MAR 2016)* or SCP-FSS-001-*S Instructions Applicable to Successful FSS Program Contractors*, as applicable.

(d) Offerors *submitting* an offer under Schedule 70 must also comply with the following:

I. Section I Administrative/Contract Data

(1) All proposed products must comply with the Trade Agreements Act (TAA). It is the responsibility of the Offeror to determine TAA compliance. When an item consists of components from various countries and the components are assembled in an additional country, the test to determine country of origin is "substantial transformation" (reference FAR 25.001(c)(2))). The Offeror may also request an opinion from a third-party expert or make the determination itself. Offerors can go to The Office of Regulations and Rulings within U.S. Customs and Border Protection (CBP), which is the Federal agency responsible for making final substantial transformation determinations(reference 19 CFR Part 177 Subpart B). CBP's determinations or opinions are based upon tariff laws . The Internet address for CBP is: https://www.cbp.gov/. The Offeror should keep this requirement in mind when completing the TAA certification section of its SAM registration. When evaluating offers, the contracting officer will rely on the representations and certifications of the Offeror and will not make substantial transformation determinations.

(2) If the Offeror is not the manufacturer of the product(s) being proposed, an acceptable Letter of Commitment/Supply must be provided. See clause I-FSS-644 Dealers and

Suppliers in the Basic Solicitation and the letter requirements. Failure to provide acceptable Letters of Commitment/Supply may result in rejection of the offer. See Letter of Supply Template for required language.

(3) 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.

II. Section II Technical Proposal:

The Offeror shall address the technical factors as described below for specific Special Items Numbers (SINs), where applicable:

(1) FACTOR 1: Corporate Experience: See SCP-FSS-001-N

(2) FACTOR 2: Past Performance: See SCP-FSS-001-N

(3) FACTOR 3: Quality Control: See SCP-FSS-001-N

(4) FACTOR 4: Relevant Project Experience: The Offeror must submit a narrative demonstrating relevant project experience. A narrative is required for each proposed total solution or service SIN, (this includes, but is not limited to, SIN 132-51 -Information Technology Professional Services, **SIN 132-45 - Highly Adaptive Cybersecurity Services**, SIN 132-56 – Health Information Technology Services, SIN 132-60f - Identity and Access Management Professional Services, SIN 132-41 Earth Observation Solutions) and SIN 132-20 Automated Contact Center Solutions. The narrative must include the following:

(i) The narrative must include a description of three (3) relevant projects, not to 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. For companies with less than two years of corporate experience, Offeror shall submit relevant projects of key personnel.

Each project description must also address the following elements:

(A) Detailed description of SIN-relevant work performed and results achieved.

(B) Methodology, tools, and/or processes utilized in performing the work.

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

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

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

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

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.

(ii) The following SINs have additional requirements that shall be addressed in the Relevant Project Experience narrative:

(A) SIN 132-54 Commercial Satellite Communications (COMSATCOM), SIN 132-55 Commercial Satellite Communications (COMSATCOM) Subscription Services, and SIN 132-56 Health Information Technology Services.

(1) Address requirements in CI-FSS-152-N Additional Evaluation Factors for New Offerors Under Schedule 70 or CI-FSS-152-S Additional Evaluation Factors for Successful FSS Program Contractors Under Schedule 70.

(2) Address requirements in CI-FSS-055 Commercial Satellite Communication (COMSATCOM) Services.

(B) SINs 132-60A – 132-60F Identity, Credential and Access Management (ICAM).

(1) Address requirements in CI-FSS-152-N Additional Evaluation Factors for New Offerors Under Schedule 70 or CI-FSS-152-S

Additional Evaluation Factors for Successful FSS Program Contractors Under Schedule 70.

(2) Address requirements in CI-FSS-052 *Authentication of Products and Services*.

(C) SIN 132-50 Training - The narrative must include the following:

(1) Course names, brief description, length of course, type of training, location (on or off customer site) and 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.

* Note that commercially available products under this solicitation may be covered by the Energy Star or Electronic Product Environmental Assessment Tool (EPEAT) programs. For applicable products, offerors are encouraged to offer Energy Star-qualified products and EPEAT-registered products, at the Bronze level or higher. If offerors opt to offer Energy Star or Electronic Product Environmental Assessment Tool (EPEAT) products then they shall identify by model which products offered are Energy Star-qualified and EPEAT-registered, broken out by registration level of bronze, silver, or gold.

(D) SIN 132-56 Health Information Technology Services

1) Address requirements in CI-FSS-152-N Additional Evaluation Factors for New Offerors Under Schedule 70 or CI-FSS-152-S Additional Evaluation Factors for Successful FSS Program Contractors Under Schedule 70

(E) SIN 132-20 Automated Contact Center Solutions

1) Address requirements in CI-FSS-152-N Additional Evaluation Factors for New Offerors Under Schedule 70 or CI-FSS-152-S Additional Evaluation Factors for Successful FSS Program Contractors Under Schedule 70.

(5) Factor 5: ORAL TECHNICAL EVALUATION:

(i) This evaluation factor is for offerors proposing services under SIN 132-45 - Highly Adaptive Cybersecurity Services (HACS).

(ii) ORAL TECHNICAL EVALUATION OVERVIEW: 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 subcategory as set forth in this solicitation, excepting those service components awarded through the submission of the Service Self-Attestation (see SCP-FSS-004 section (d)(II)(5)(ii)(E)).

An offeror may only be awarded the HACS SIN 132-45- 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" subcategories, additional questions related to those areas will be asked during the HACS Oral Technical Evaluation.

(A) 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 five (5) subcategories. The base HACS SIN Oral Technical Evaluation consists of questions related to the 3 subcategories of, High Value Asset Assessments, Risk and Vulnerability Assessments and Penetration Testing. One (1) hour and 40 minutes is allotted for the base HACS SIN Oral Technical Evaluation. The evaluation will be stopped precisely after 1 hour and 40 minutes. Should the offer elect to be considered for the additional subcategories of Incident Response and Cyber Hunt, an additional 10 minutes will be allotted for each of those subcategories. The total base evaluation session is expected to last up to one (1) hour and 40 minutes, depending on the number of subcategories the offeror is proposing. 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.

(B) ORAL TECHNICAL EVALUATION SCHEDULING: The TEB will contact the offeror's authorized negotiator or the signatory of the 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.

(C) PROHIBITION OF ELECTRONIC RECORDING OF THE ORAL TECHNICAL EVALUATION: The offeror may not record or transmit any of the oral evaluation process. 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.

(D) 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 be acceptable 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.

(E) HIGH VALUE ASSET (HVA) ASSESSMENTS SUBCATEGORY PLACEMENT: Any offeror previously awarded all of the following four SINs: 132-45A Penetration Testing, 132-45B Incident Response, 132-45C Cyber Hunt, and 132-45D Risk and Vulnerability Assessment, shall not be subject to a HACS SIN oral technical evaluation, as long as they provide in the modification package to the GSA Contracting Officer a Service Self-Attestation acknowledging its ability to perform Security Architecture Review (SAR) and Systems Security Engineering (SSE) services in their entirety.

(iii) Oral Technical Evaluation Procedure

The offeror will be evaluated on its 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 evaluation criteria is listed below.

(iv) 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 it 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 an acceptable/unacceptable basis. The rating definitions provided below will be used for the evaluation of the offeror's responses to questions during the oral evaluation.

TECHNICAL RATINGS

Rating	Definition
Acceptable	**The proposal meets the minimum requirements of the solicitation.**
Unacceptable	**The proposal does not meet the minimum requirements of the solicitation.**

(6) Factor 6 Product Qualification Requirements for SIN 132-44 CDM Tools SIN

(i) SIN 132-44 CDM Tools SIN Background

(a) General Services Administration (GSA) is providing a Continuous Diagnostics and Mitigation (CDM) Tools SIN as part of the CDM Program to safeguard, secure, and strengthen cyberspace and the security posture of networks. The CDM Tools SIN is a government-wide contracting solution to provide a consistent set of continuous diagnostics and mitigation tools. The SIN enhances the ability of offerors to bring new and innovative solutions to the CDM Program through continuous technology refresh.

(ii) Product Qualification Requirements

(a) The hardware and software products, and associated services under SIN 132-44 shall undergo a product qualification process, outside the solicitation, by a third party to be added to the CDM Approved Products List (APL). Qualification requirements and procedures for the evaluation of products and associated services are set forth in a separate document posted at http://gsa.gov/cdm (along with the CDM APL Submission Form to be completed by the offeror for APL submission). In addition to the evaluation of other technical and non-technical factors, only items on the approved CDM APL (received by GSA) shall be included as part of offering for this

SIN. New offers for hardware, software, and associated services are required to go through the product qualification process prior to submission to GSA for Schedule 70 contract or modification consideration. Offerors must submit Commercial Supplier Agreement 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) for approval prior to submitting an offer or modification for CDM APL approval.

The SIN offerings are organized by CDM capabilities into 5 subcategories. Offerings may be in more than one category. Offerors should identify the subcategory (on the CDM APL Submission Form and Price Proposal Template for the offer and/or modification).

GSA is responsible for the final approval to add the CDM Tools SIN and associated offerings or offer award of the SIN and associated offerings. This includes Commercial Supplier Agreement Terms, and Letters of Supply (LOS) if not the original manufacturer, and in accordance with GSA's solicitation requirements.
Offerors and existing contractors applying under this SIN must submit for Commercial Supplier Agreement Terms approval prior to submitting an offer or modification to GSA. Commercial Supplier Agreement Terms shall be sent to schedule70cdmsin@gsa.gov for review and approval.

III Section III - Price Proposal

The Offeror must address additional pricing requirements as described below:

(i) The Offeror must address additional pricing requirements below as described below: The offeror has the option to propose separate rates for "domestic" versus "overseas" and/or "customer facility" versus "contractor facility" if there are variations in costs that depend on where the work is performed. Rates proposed in this manner must be clearly labeled as such.

(A) For each proposed labor category, the offeror must provide a detailed position description. Position descriptions are to be uploaded to eOffer, and must include functional responsibilities, minimum years of experience, minimum educational/degree requirements, and any applicable training or certification requirements. If it is the offeror's standard commercial practice to substitute experience for education, explain the methodology in use (e.g., five years of experience equates to a BA/BS degree). Once the contract is awarded, these descriptions will become part of the Authorized Federal Supply Schedule Price List. It is the responsibility of the Offeror to post the approved descriptions to GSA *Advantage!*®.

(B) Proposed prices for services must represent fully-burdened rates inclusive of all cost factors (e.g., direct labor, indirect labor, G&A, profit, and IFF). (See Proposal Price Template – Labor Categories spreadsheet tab.)

(ii) The Offeror must submit a Professional Compensation Plan in accordance with clause 52.222-46 *Evaluation of Compensation for Professional Employees*. Submission of the general compensation practices printed in the offeror's employee handbook is often sufficient. Individual compensation disclosure (by Employee Name) is not required.

(iii) The Offeror must submit a copy of its policy that addresses uncompensated overtime, in accordance with clause 52.237-10 *Identification of Uncompensated Overtime*.

(iv) The Offeror must submit a copy of its proposed Authorized Federal Supply Schedule Pricelist for the General Purpose Commercial Information Technology, Equipment, Software and Services Schedule (see clause I-FSS-600 *Contract Price Lists.*

(v.) Service Contract Act: Applicable to this solicitation (Service Contract Act 52.222-41, and related clauses 52.222-42, 52.222-43, and 52.222-49).

(A) The Service Contract Act (SCA) applies to all nonprofessional services to be provided under this Schedule except for any pricing offered for services outside of the United States. The SCA index of applicable wage determinations for this solicitation and resultant contract are shown in FedBizOpps document, "SCA Index of Wage Determinations." The full-text version of each wage determination can be viewed at https://www.wdol.gov. Some of the proposed labor categories may be subject to the SCA (usually nonprofessional categories). As such, the offeror should verify that its proposed base rates and fringe benefit rates for these labor categories meet or exceed the SCA wage determination rates and fringe benefits for the areas included in the geographic scope of the contract (i.e., nationwide); the offeror will be required to comply with applicable SCA wage determination rates and fringe benefits regardless of the price proposed and awarded on any resultant Schedule contract. The offeror may be required to submit supporting documentation for the proposed rates that will allow the contracting officer to conduct cost analysis to determine that offered prices are fair and reasonable.

(B) Schedule contractors must comply with the base rate and fringe benefit rate requirements of the prevailing rate SCA Wage Determination (WD) Revision Number currently incorporated into the GSA Schedule contract. No prevailing rate WD may be incorporated into a task order as the order may then be in conflict with the Schedule contract terms and conditions.

However, WDs based on collective bargaining agreements (CBAs) may be incorporated into a task order if the task order is found to be a successor contract as used in FAR Subpart 22.10; a CBA WD would be applicable only to the task order it is incorporated into and no other orders under that Schedule contract.

(C) In the price proposal, indicate which proposed labor categories are subject to the SCA by placing a double asterisk (**) next to the labor category name.

(D) The following paragraph is meant to be instructive and NOT to be copied as part of proposed Schedule pricing:

For all the offeror's identified SCA-eligible labor categories, map them to the SCA-equivalent labor category title (titles/descriptions available at https://www.wdol.gov - click on the "library" link, then download the SCA Directory of Occupations, 5th Edition). Also identify the WD# that the labor categories in your offer are predicated on. Note that the applicable revision number for any Wage Determination number is the revision number identified in the solicitation index of wage determinations.

(E) There are two possible strategies for determining price adjustments under SCA-eligible labor categories. All price adjustments under SCA-eligible labor categories shall be in accordance with clause 52.222-43.

52.222-43 Fair Labor Standards Act and Service Contract Act Price Adjustment (Multiple Year and Option Contracts). Price adjustments for SCA-applicable labor categories shall be in accordance with clause 52.222-43 Fair Labor Standards Act and Service Contract Act Price Adjustment (Multiple Year and Option Contracts). When a modification is issued to all contract holders incorporating a revised index of wage determinations, contractors shall notify the contracting officer of any increase/decrease claimed under clause 52.222-43 within 30 calendar days after receipt of the modification.

In addition to clause 52.222-43, one of the following two methods of escalation will be awarded.

Method 1: An escalation method is negotiated prior to award in accordance with the clause I-FSS-969 *Economic Price Adjustment - FSS Multiple Award Schedule*, utilizing any of the methods available in the solicitation under that clause.

OR

Method 2: When the offered prices are based upon a commercial price list, only revisions in the commercial price list will enable the contractor to revise Schedule contract prices. Schedule contract price increases will be allowed only in accordance with clause 552.216-70 *Economic Price Adjustment - FSS Multiple Award Schedule Contracts*.

Regardless of the method used, the contractor must ensure that within 30 calendar days after the effective date of any contract modification to revise pricing based on changes in the applicable wage determination(s), the contractor's electronic catalog is updated on GSA *Advantage!*®.

Note 1: The contractor will not automatically be allowed an increase in prices based solely on new wage determinations.

Note 2: Reference Code of Federal Regulations, Title 29, Labor, Subtitle A Office of the Secretary of Labor, Part 4 Labor Standards for Federal Service Contracts, Subpart D Compensation Standards, paragraph 4.161 Minimum monetary wages under contracts exceeding $2,500, which states: "No change in the obligation of the contractor or subcontractor with respect to minimum wages will result from the mere fact that higher or lower wage rates may be determined to be prevailing for such employees in the locality after the award and before completion of the contract."

(F) Utilize the module in eOffer to submit SCA information in the following format

(labor categories shown are for example purposes only):

SCA Matrix		
SCA Eligible Contract Labor Category	SCA Equivalent Code Title	WD Number
Secretary	01115 General Clerk I	052059
Driver	31361 Truckdriver, Light Truck	052059

Engineering Technician	29081 Engineering Technician I	052059
Administrative Assistant	01011 Accounting Clerk I	052059

(G) Insert the following language below the above SCA matrix and insert both (matrix and language) at the end of the proposed GSA price list.

"The Service Contract Act (SCA) is applicable to this contract and it includes SCA applicable labor categories. The prices for the indicated (**) SCA labor categories are based on the U.S. Department of Labor Wage Determination Number(s) identified in the SCA matrix. The prices awarded are in line with the geographic scope of the contract (i.e. nationwide)."

----- Beginning Regulation -----

CI-FSS-152-N ADDITIONAL EVALUATION FACTORS FOR NEW OFFERORS UNDER SCHEDULE 70 (AUG 2017)

(a) The Government will consider award to an offeror who has been determined to be responsible, whose offer conforms to all solicitation requirements, who is determined technically acceptable, who has acceptable past performance, and whose prices are determined fair and reasonable.

(b) All technical evaluation factors will be reviewed, evaluated, and rated acceptable or unacceptable based on the criteria listed below. 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.

I. TECHNICAL EVALUATION FACTORS:

(1) FACTOR 1: Corporate Experience: See SCP-FSS-001-N

(2) FACTOR 2: Past Performance: See SCP-FSS-001-N

(3) FACTOR 3: Quality Control: See SCP-FSS-001-N

(4) FACTOR 4: Relevant Project Experience: See SCP-FSS-004. Additional requirements are:

(i.) SIN 132-41 Earth Observation Solutions, **SIN 132-45- Highly Adaptive Cybersecurity Services**, SIN 132-51 IT Professional Services, **SIN 132-53 Wireless Mobility Solutions,** SIN 132-60f Identity Access Management (IAM) Professional Services and SIN 132-20 Automated Contact Center Solutions only.

(A) Provide a description of the offeror's experience in the professional information technology services offered under SIN 132-20, SIN 132-41, **132-45**, SIN 132-51, **SIN 132-53** and/or SIN 132-60f. Describe three 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. For SIN 132-60f, two of the three projects described must be prior Federal Government application deployment projects for public-facing IT systems. Each completed example shall have been completed within the last two years.

For SIN 132-20, narratives must include the following, where applicable: 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.

For 132-41, the offeror shall provide a narrative of services provided or a project where products were provided.

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

(B) Within the four-page limitation for each project narrative, offerors shall outline the following for proposed SINs: SIN 132-20, SIN 132-41, **SIN 132-45**, 132-51, **SIN 132-53** and 132-60f:

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

2) Outline how the project or projects are related to the proposed SIN(s).

3) Submit summary of the final deliverables for the noted project or projects.

4) Offerors shall demonstrate that the tasks performed are of a similar complexity to the work solicited under this solicitation.

5) Provide the following information for each project submitted:

i) Project/Contract Name;

ii) Project Description;

iii) Dollar Amount of Contract;

iv) Project Duration, which includes the original estimated completion date and the actual completion date; and

v) Point of Contact and Telephone Number.

(ii.) SIN 132-54, Commercial Satellite Communications (COMSATCOM) Transponded Capacity and/or SIN 132-55, COMSATCOM Subscription Services

(A) Provide a description of the offeror's experience delivering COMSATCOM services as described in CI-FSS-055 *Commercial Satellite Communication (COMSATCOM) Services*. For each COMSATCOM Services SIN proposed, describe three completed or ongoing projects, similar in size and complexity to the services the vendor is proposing to offer and in sufficient detail for the Government to perform an evaluation. (NOTE: If applying for both SIN 132-54 and 132-55, describe three projects related to SIN 132-54, and another three projects related to SIN 132-55.) All completed projects shall have been completed within the last three years prior to submission of the vendor's COMSATCOM Services

SIN proposal. Performance of all completed projects shall have been found acceptable by the ordering activity. If the offeror cannot provide three projects, it may provide additional documentation to substantiate project experience to be evaluated by the contracting officer.

(B) Within the four-page limitation for each project narrative, the offeror shall include the following information:

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

2) Outline how the project is related to the proposed COMSATCOM Services SIN.

3) Demonstrate that the tasks performed are of a similar size, scope, and complexity to the work solicited under this solicitation.

4) Provide the following information for each project submitted:

i) Project/Contract Name;

ii) Project Description;

iii) Dollar Amount of Contract;

iv) Project Duration, which includes the original estimated completion date and the actual completion date; and

v) Point of Contact and Telephone Number.

(iii.) Information Assurance Minimum Security Controls Compliance for SIN 132-54, Commercial Satellite Communications (COMSATCOM) Transponded Capacity Services and SIN 132-55, COMSATCOM Subscription Services only.

(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

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 GSA SATCOM Services Program Management Office website (http://www.gsa.gov/portal/content/122627).

(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.

(iv.) SIN 132-56 Health Information Technology Services

(A) Provide a description of the offeror's experience in the Health information technology services offered under SIN 132-56. Describe three 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.
Each completed example shall have been completed within the last three years. All examples of completed services shall have been found to be acceptable by the ordering activity.

(B) Within the four-page limitation for each project narrative, offerors shall outline the following for proposed SIN 132-56:

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

2) Outline how the project or projects are related to the proposed Health IT SIN.

3) Submit summary of the final deliverables for the noted project or projects.

4) Offerors shall demonstrate that the tasks performed are of a similar complexity to the work solicited under this solicitation.

5) Provide the following information for each project submitted:

i) Project/Contract Name;

ii) Project Description;

iii) Dollar Amount of Contract;

iv) Project Duration, which includes the original estimated completion date and the actual completion date; and

v) Point of Contact and Telephone Number.

(v.) Project Experience for Authentication Products and Services (Homeland Security Presidential Directive 12 (HSPD-12) Only): 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:

(A) SIN 132-60a: Offerings must include policy-compliant agency setup, testing, credential issuance, subscriber customer service account management, revocation, and credential validation as part of the basic service. Technical evaluation criteria are -

1) Successful completion of Level 1 Credential Assessment - Include Assessment Report

2) Successful completion of applicable interoperability testing - Include Test Report

(B) SIN 132-60b: Offerings must include policy-compliant agency setup, testing, identity proofing, credential issuance, subscriber customer service account management, revocation, and credential validation as part of the basic service. Technical evaluation criteria are -

1) Successful completion of Level 2 Credential Assessment - Include Assessment Report

2) Successful completion of applicable interoperability testing - Include Test Report

(C) SIN 132-60c: Offerings must include policy compliant ID proofing, Credential issuance, continued account management, revocation, and certificate validation as part of the basic service. Technical evaluation criteria are -

1) Successful completion of Level 3 and 4 Credential Assessment - Include Assessment Report

2) 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.

3) Common criteria for other Certification Authorities cross-certified by the Federal Bridge

(D) SIN 132-60d: Offerings must be -

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

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

(E) SIN 132-60e: Offerings must include 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. Technical evaluation criteria are -

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

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

(F) SIN 132-60f: Technical evaluation criteria are -

1) 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.

(5) Factor 5 - ORAL TECHNICAL EVALUATION: **See SCP-FSS-004. New offerors proposing services under SIN 132-45, Highly Adaptive Cybersecurity Services additional requirements are:**

(i) This evaluation factor is for offerors proposing services under SIN 132-45 - Highly Adaptive Cybersecurity Services (HACS).

(ii) ORAL TECHNICAL EVALUATION OVERVIEW: 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 subcategory as set forth in this solicitation, excepting those service components awarded through the submission of the Service Self-Attestation (see SCP-FSS-004 section (d)(II)(5)(ii)(E)).
An offeror may only be awarded the HACS upon successful completion of the HACS SIN oral technical evaluation. If the offeror elects to be cataloged under the "Cyber Hunt" and/or "Incident Response" subcategories, additional questions related to those areas will be asked during the HACS Oral Technical Evaluation.

(A) ORAL TECHNICAL EVALUATION CONSTRAINTS: The offeror shall identify up to five (5) key personnel, by name and association with the offeror, who will field questions during the oral technical evaluation. The HACS SIN consists of five (5) subcategories. The base HACS SIN Oral Technical Evaluation consists of questions related to the three (3) subcategories of High Value Asset Assessments, Risk and Vulnerability Assessments and Penetration Testing. One (1) hour and 40 minutes is allotted for the base HACS SIN Oral Technical Evaluation. The evaluation will be stopped precisely after one (1) hour and 40 minutes. Should the offer elect to be considered for the additional subcategories of Incident Response and Cyber Hunt, an additional 10 minutes will be allotted for each of those subcategories. The total base evaluation session is expected to last up to one (1) hour and 40 minutes, depending on the number of subcategories the offeror is proposing. 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.

(B) ORAL TECHNICAL EVALUATION SCHEDULING: The TEB will contact the offeror's authorized negotiator or the signatory of the 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.

(C) PROHIBITION OF ELECTRONIC RECORDING OF THE ORAL TECHNICAL EVALUATION: The offeror may not record or transmit any of the oral evaluation process. 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.

(D) 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 be acceptable 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.

(E) HIGH VALUE ASSET (HVA) ASSESSMENTS SUBCATEGORY PLACEMENT: Any offeror previously awarded all of the following four SINs: 132-45A Penetration Testing, 132-45B Incident Response, 132-45C Cyber Hunt, and 132-45D Risk and Vulnerability Assessment, shall not be subject to a HACS SIN oral technical evaluation, as long as they provide in the modification package to the GSA Contracting Officer a Service Self-Attestation acknowledging its ability to perform Security Architecture Review (SAR) and Systems Security Engineering (SSE) services in their entirety.

(iii) Oral Technical Evaluation Procedure

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:

(iv) 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 it 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 an acceptable/unacceptable basis. The rating definitions provided below will be used for the evaluation of the offeror's responses to questions during the oral evaluation.

TECHNICAL RATINGS

Rating	Definition

Acceptable	**The proposal meets the minimum requirements of the solicitation.**
Unacceptable	**The proposal does not meet the minimum requirements of the solicitation.**

(6) FACTOR 6: Product Qualification Requirements for SIN 132-44. See SCP-FSS-004.

----- Ending Regulation -----

Part I - GOODS & SERVICES

132-53 --- Wireless Mobility Solutions - SUBJECT TO COOPERATIVE PURCHASING

~~132-53 --- Wireless Services - SUBJECT TO COOPERATIVE PURCHASING Wireless Services, including but not limited to Wireless Telecommunications Carriers and Telecommunication Resellers.~~

~~Please see the additional terms and conditions applicable to this Special Item Number (SIN) found in a separate attachment to the Solicitation. These terms and conditions do not contain specific and negotiated contractual language for this SIN. The Schedule contractor may have submitted additional information to complete the "fill-in" to the terms and conditions. The ordering activities shall request the Schedule contractors to submit these additional contract terms and conditions for this applicable SIN when responding to an order.~~

~~Cellular service is one of several services excluded from the World Trade Organization Government Procurement Agreement and the other Free Trade Agreement executed by the United States Government. See FAR 25.401(b). The wireless service offered under this contract has been determined by the GSA Schedule Contracting Officer to be domestic in origin. See FAR 25.402(a)(2).~~

~~All Nationwide Business Plans under this contract may include no-cost service enabling devices (including, but not limited to cell phones and shall be offered to the general public at no-cost), bundling the devices with cellular service. The service enabling devices are offered on as~~

available basis and may or may not be domestic end products or end products of a designated country. The no-cost devices are not available through this contract apart from ordering cellular service. Equipment is available for purchase under SIN 132-8 or 132-9 or for lease under SIN 132-3 or short term rental under 132-4, where TAA is applicable.

As cellular service is excluded from TAA coverage, GSA has used the group offer analysis provided by FAR 25.503(c)(1) and (2) to determine that for the bundled wireless service with no-cost service enabling device, the value of the domestic end product exceeds 50 percent of the total proposed price of the group, therefore the bundled cellular service and service enabling device group offer is evaluated as domestic and eligible for award.

Ordering activities may request from Schedule contractors their awarded End User License Agreements (EULAs) or Terms of Service (TOS) Agreements, which will assist the ordering activities with reviewing the terms and conditions and additional products, services, and prices which may be included. Note: Commercially available products under this solicitation may be covered by the Energy Star or Electronic Product Environmental Assessment Tool (EPEAT) programs. For applicable products, offerors are encouraged to offer Energy Star-qualified products and EPEAT-registered products, at the Bronze level or higher. If offerors opt to offer Energy Star or Electronic Product Environmental Assessment Tool (EPEAT) products then they shall identify by model which products offered are Energy Star-qualified and EPEAT-registered, broken out by registration level of bronze, silver, or gold. Visit the Green Procurement Compilation, www.sftool.gov/greenprocurement for a complete list of products covered by these programs.

NOTE: Exception: According to SBA standards NAICS code 541519 has the dollar value standard of $27.5 million except if you are a Value Added Reseller (150 employee standard). For more information,please visit
http://www.naics.com/naicswp2014/wp-content/uploads/2014/10/2014-Size_Standards_Table.pdf

Sales: $439,418,331
Sales Period: Oct 1, 2016 to Sep 30, 2017
Cooperative Purchasing: Yes
Set Aside: No
FSC/PSC Code : D304
Maximum Order : $500,000

NAICS

Number	Description	Business Size Standard
517312	Wireless Telecommunications Carriers (except Satellite)	1500 employees
517911	Telecommunications Resellers	1500 employees

~~517919~~	~~All Other Telecommunications~~	~~$32.5 million~~
~~541519~~	~~Other Computer Related Services~~	~~$27.5 million~~

~~SubSIN Categorie(s):~~

~~FSC/PSC Class D304 IT AND TELECOM- TELECOMMUNICATIONS AND TRANSMISSION~~
~~• Cellular/PCS Voice Services~~
~~• Paging Services~~

The IT Schedule 70 SIN for Wireless Mobility Solutions includes a variety of services that address the mobility needs of government agencies. The following sub-categories associated with the Wireless & Mobile Services SIN 132-53 include but are not limited to:

Sub-Category Descriptions

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). The wireless service offered under this contract has been determined by the GSA Schedule Contracting Officer to be CONUS and OCONUS in origin. See FAR 25.402(a)(2).

Wireless service plans offered by contractors may include no-cost Service Enabling Devices (SEDs) bundled together and offered to the ordering government agency for a monthly recurring charge (MRC). 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. A SED shall be provided only as needed to deliver a service that is acquired under an

order. 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. As mobile wireless service is excluded from TAA coverage, GSA has used the group offer analysis provided by FAR 25.503(c)(1) to determine that for the bundled wireless service with a SED, the value of the domestic end product exceeds 50 percent of the total proposed price of the group, therefore the bundled cellular service and SED group offer is evaluated as domestic and eligible for award. The SEDs are not available through this contract apart from ordering the services under this SIN.

Ordering activities may request from IT Schedule 70 contractors their awarded End User License Agreements (EULAs) or Terms of Service (TOS) Agreements, which will assist the ordering activities with reviewing the terms and conditions as well as reviewing additional products, services, and prices which may be included.

NOTE 1: Commercially-available products under this solicitation may be covered by the Energy Star or Electronic Product Environmental Assessment Tool (EPEAT) programs. For applicable products, offerors are encouraged to offer Energy Star-qualified products and EPEAT-registered products, at the Bronze level or higher. If offerors opt to offer Energy Star or Electronic Product Environmental Assessment Tool (EPEAT) products then they shall identify by model which products offered are Energy Star-qualified and EPEAT-registered, broken out by registration level of bronze, silver, or gold. Visit the Green Procurement Compilation, www.sftool.gov/greenprocurement for a complete list of products covered by these programs.

NOTE 2: The Transactional Data Reporting (TDR) Rule requires vendors to report the price the Federal Government paid for an item or service purchased through GSA acquisition vehicles. The TDR PILOT DOES NOT APPLY TO THIS SIN, EXCEPT if a TDR-covered SIN(s) is proposed as part of your total offering to GSA (e.g. offer 132-51 and 132-8). If both TDR and NON-TDR SINs are offered, then the entire contract is subject to TDR and the Price Reduction Clause (PRC) and Commercial Sales Practice (CSP) requirements are removed for the entire contract. If NON-TDR SIN(s) are offered only, then the offering will be subject to the PRC and CSP.

NOTE 3: Exception: According to SBA standards NAICS code 541519 has the dollar value standard of $27.5 million except if you are a Value-Added Reseller (150 employee standard). For more information, please visit - http://www.naics.com/naicswp2014/wp-content/uploads/2014/10/2014-Size_Standards_Table.pdf

Note 5: Please see the additional terms and conditions applicable to this Special Item Number (SIN) found in attachment to solicitation [#_Critical Information Specific to Schedule 70]. Terms and conditions described above do not contain specific and negotiated contractual language for this SIN. The Schedule contractor may have submitted additional information to complete the "fill-in" to the terms and conditions. The ordering activities shall request the Schedule contractors to submit these additional contract terms and conditions for this applicable SIN when responding to an order.

Sales: $737,574,164
Sales Period: Oct 1, 2016 to Sep 30, 2017
Cooperative Purchasing: Yes
Set Aside: No
FSC/PSC Code : D304
Maximum order- $500,000

NAICS

Number	Description	Business Size Standard
517312	Wireless Telecommunications Carriers (except Satellite)	1500 employees
517911	Telecommunications Resellers	1500 employees
517919	All Other Telecommunications	$32.5 million
541519	Other Computer Related Services	$27.5 million

FSC/PSC Class D304 IT AND TELECOM- TELECOMMUNICATIONS AND TRANSMISSION

- Cellular/PCS Voice Services
- Paging Services

FSC/PSC Class D305 IT AND TELECOM- TELEPROCESSING, TIMESHARE, AND CLOUD COMPUTING

FSC/PSC Class D307 IT AND TELECOM - IT STRATEGY AND ARCHITECTURE

FSC/PSC Class D310 IT AND TELECOM - CYBER SECURITY AND DATA BACKUP

FSC/PSC Class D314 IT AND TELECOM - SYSTEM ACQUISITION SUPPORT

FSC/PSC Class D317 IT AND TELECOM- WEB-BASED SUBSCRIPTION

- Web-Based Subscription
- Creation/Retrieval of IT Related Data Services
- Creation/Retrieval of Other Information Services

FSC/PSC Class D318 IT AND TELECOM - INTEGRATED HARDWARE/SOFTWARE/SERVICES SOLUTIONS, PREDOMINANTLY SERVICES

FSC/PSC Class D399 IT AND TELECOM- OTHER IT AND TELECOMMUNICATIONS

- Other IT and Telecommunications Services

---

132 61 --- Public Key Infrastructure (PKI) Shared Service Providers (PKI SSP) Program

~~This program provides PKI services and digital certificates for use by Federal employees and contractors to the Federal Government in accordance with the~~ The Federal Government established the Public Key Infrastructure (PKI) Shared Service Provider (SSP) Program to ensure that Digital Certificate Service Providers are compliant with the Federal Information Security Management Act (FISMA) and all associated Federal laws, ordinances, regulations, policies, and/or agreements to include the X.509 Certificate 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.

Please see the additional terms and conditions applicable to this Special Item Number (SIN) found in a separate attachment to the Solicitation. These terms and conditions do not contain specific and negotiated contractual language for

this SIN. The Schedule contractor may have submitted additional information to complete the "fill-in" to the terms and conditions. The ordering activities shall request the Schedule contractors to submit these additional contract terms and conditions for this applicable SIN when responding to an order.

Ordering activities may request from Schedule contractors their awarded End User License Agreements (EULAs) or Terms of Service (TOS) Agreements, which will assist the ordering activities with reviewing the terms and conditions and additional products and services and prices which, may be included.

Exception: According to SBA standards NAICS code 541519 has the dollar value standard of $27.5 million except if you are a Value Added Reseller (150 employee standard). For more information, please visit
http://www.naics.com/naicswp2014/wp-content/uploads/2014/10/2014-Size_Standards_Table.pdf

Sales: $7,165,701
Sales Period: Oct 1, 2016 to Sep 30, 2017
Cooperative Purchasing: Yes
Set Aside: No
FSC/PSC Code: D399
Maximum Order: $1,000,000

NAICS

Number	Description	Business Size
541519	Other Computer Related Services	$27.5 million

SubSIN Categorie(s):

FSC/PSC Class D399 IT AND TELECOM- OTHER IT AND TELECOMMUNICATIONS

- Digital Signature Certificates
- Key Management (Encryption) Certificates
- Personal Identity Verification (PIV) Authentication Certificates
- Public Key Infrastructure (PKI) Professional Services
- Shared Services Providers (SSP)
- Smart Card Authentication Certificates

X.509 Digital Certificate Products and accompanying PKI Services for internal use in Federal agencies and systems. This facilitates physical and electronic access to government facilities and networks by authorized personnel using public key

infrastructure/digital signature technology that meets the U.S. Federal Public Key Infrastructure (PKI) Common Policy Framework, and is a key enabler of identity assurance within the Federal sector for access control protecting Federal networks and information systems from unauthorized access, interception, and tampering.

NOTE TO FEDERAL AGENCIES: 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 contractors (including contractor employees) 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: Personal Identity Verification (PIV) of Federal Employees and Contractors ~~on February 25, 2005 or later version~~. FIPS 201 requires that the digital certificates incorporated into PIV ~~the Personal Identity Verification identity~~ credentials comply with the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework.

The Federal Government has established the PKI Shared Service Provider Program to insure that Digital Certificate Service Providers are compliant with the X.509 Certificate 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 this program. Federal agencies are advised that they may only procure X.509 digital certificates and services ~~for internal use~~ that meet the requirements established in FIPS 201.