

## **SIGNIFICANT CHANGES DOCUMENT**

### **Descriptive Title**

Schedule 70\_MassModification\_Health IT SIN Significant Changes

### **Disclaimer Language**

“DISCLAIMER: GSA FAS is posting this notification of a planned solicitation refresh or mass modification as a courtesy to industry. All comments on the attached DRAFT document must be submitted in the “Comments” section below within ten (10) business days of this posting. Comments provided elsewhere or after 10 business days will not be considered. GSA FAS will consider all relevant comments and make changes to the DRAFT as appropriate, but will not issue a formal response to industry comments or related inquiries. Interested parties should review the final version of the solicitation refresh or mass modification closely for additional changes made to this DRAFT.”

### **Purpose of Planned Action**

IT Schedule 70 is proposing a new Special Item Number (SIN) for Health IT to assist customer agencies in procuring Health IT services by clearly differentiating them from other IT related services currently available under the program.

Over the last six years, healthcare has been the fastest growing segment in the federal government and commercial markets. Health Information Technology (Health IT) makes it possible for healthcare providers to manage patient care better through the secure use and sharing of health information. The Health IT market is currently valued at \$21.9 billion annually and is forecasted to grow at 7.4 percent reaching \$31.3 billion by 2017 (Healthcare IT News). Given the current focus on military health and civilian healthcare reform, Health IT has become a valued market for the General Services Administration (GSA) and its customers.

GSA, Federal Acquisition Service (FAS), Integrated Technology Services (ITS) provides commercial IT products and services through IT Schedule 70. The \$15 billion IT Schedule 70 Program is the vehicle through which agency customers can access the latest technology solutions, making it critical for requiring GSA to adapt to its customers' new and growing services.

### **Summary of Planned Changes**

Below is a high-level description of significant changes planned for the upcoming mass modification identified above. The full text for any new or updated clauses and provisions not currently available in the FAR or GSAM is provided at the end of this document.

1. IT Schedule 70 is proposing a new Special Item Number (SIN) for Health IT to assist customer agencies in procuring Health IT services by clearly differentiating them from other IT related services currently available under the program.

### **Benefits to Industry Partners**

The new Health IT SIN will provide industry partners the opportunity to differentiate their Health IT services offerings from other IT related services under existing services; therefore, allowing industry partners to stand out to agencies seeking Health IT services.

### **SWS Solicitation Special Item Number Description:**

#### **132-56 --- Health Information Technology Services - SUBJECT TO COOPERATIVE PURCHASING**

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: 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.

NOTE: This SIN is limited to Health IT services only. Software and hardware products are out of scope.

2. In 2015, GSA's Senior Procurement Executive issued a class deviation that implements Section 743 of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) for GSA contracting activities. Section 743 prohibits agencies from obligating funds to entities that require their employees (or subcontractors) to sign internal confidentiality agreements (or similar documents) that restrict them from lawfully reporting waste, fraud, or abuse. MAS solicitations will include the provision and clause below to implement this policy until the FAR has been updated to include these requirements.

The following clause will be ADDED:

- 52.203-98, Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements—Representation (FEB 2015) (DEVIATION 2015-02)

The following provision will be ADDED:

- 52.203-99, Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements (FEB 2015) (DEVIATION 2015-02)

### **New/Updated Clauses and Provisions**

Provisions SCP-FSS-004 and CI-FSS-152-N were revised to incorporate proposal and evaluation language specific to the Health IT SIN.

-----

#### **SCP-FSS-004      SPECIFIC PROPOSAL INSTRUCTIONS FOR SCHEDULE 70 (APR 2016)**

- (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: <http://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 END USER LICENSE AGREEMENTS (EULAs), TERMS OF SERVICE (TOS) AGREEMENTS FOR SOFTWARE USE, AND/OR OTHER 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 EULA or TOS Agreement 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 EULA, TOS Agreement, and other Agreements.

## **II Section II - Technical Proposal:**

### **The Offeror must address a fourth technical factor as described below:**

(1) Factor Four – 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, SIN132-51 -Information Technology Professional Services, SIN132-56 – Health Information Technology Services and SIN 132-60f - Identity and Access Management Professional Services). 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.

---

**CI-FSS- 152-N ADDITIONAL EVALUATION FACTORS FOR NEW OFFERORS UNDER SCHEDULE 70 (OCT 2015)**

- (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 132-51 and SIN 132-60f only (IT and Identity Access Management (IAM) Professional Services)

(A) Provide a description of the offeror's experience in the professional information technology services offered under SIN 132-51 and 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. 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 two-page limitation for each project narrative, offerors shall outline the following for proposed SINs 132-51 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 two-page limitation for each project narrative, offerors shall outline the following for proposed SINs 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.**

(iiv) 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.

-----

**52.203-99 PROHIBITION ON CONTRACTING WITH ENTITIES THAT REQUIRE CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS-REPRESENTATION (FEB 2015) (DEVIATION 2015-02)**

(a) In accordance with section 743 of Division E, Title VII, of the Consolidated and Further Continuing Resolution Appropriations Act, 2015 (Pub. L. 113-235), Government agencies are not permitted to use funds appropriated (or otherwise made available) under that or any other Act for contracts with an entity that requires employees or subcontractors of such entity seeking to report fraud, waste, or abuse to sign internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting such waste, fraud, or abuse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information.

(b) The prohibition in paragraph (a) of this provision does not contravene requirements applicable to Standard Form 312, Form 4414, or any other form issued by a Federal department or agency governing the nondisclosure of classified information.

(c) *Representation.* By submission of its offer, the Offeror represents that it does not require employees or subcontractors of such entity seeking to report fraud, waste, or abuse to sign internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting such waste, fraud, or abuse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information.

**52.203-99 PROHIBITION ON CONTRACTING WITH ENTITIES THAT REQUIRE CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS (FEB 2015) (DEVIATION 2015-02)**

(a) The Contractor shall not require employees or subcontractors seeking to report fraud, waste, or abuse to sign or comply with internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting such waste, fraud, or abuse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information.

(b) The contractor shall notify employees that the prohibitions and restrictions of any internal confidentiality agreements covered by this clause are no longer in effect.

(c) The prohibition in paragraph (a) of this clause does not contravene requirements applicable to Standard Form 312, Form 4414, or any other form issued by a Federal department or agency governing the nondisclosure of classified information.

(d)(1) In accordance with section 743 of Division E, Title VII, of the Consolidated and Further Continuing Resolution Appropriations Act, 2015 (Pub. L. 113-235), use of funds appropriated (or otherwise made available) under that or any other Act may be prohibited, if the Government determines that the Contractor is not in compliance with the provisions of this clause.

(2) The Government may seek any available remedies in the event the contractor fails to comply with the provisions of this clause.