CI-FSS-152 ADDITIONAL EVALUATION FACTORS (DEC 2014)

(a) The government will consider award for an offeror who has been determined to be responsible, whose offer conforms to all solicitation requirements, is determined technically acceptable, 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 per Special Item Number (SIN) basis. A rating of "unacceptable" under any technical evaluation factor, by SIN, will result in an "unacceptable" rating overall for that SIN, in which that SIN will be rejected. Offers determined unacceptable for all proposed SIN(s) will be rejected.

I TECHNCAL EVALUATION FACTORS:

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

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

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

(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 (3) 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, one of the 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 three 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 four page limitation for each project narrative, offerors shall outline the following for proposed SIN 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 on-going 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, 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, 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) 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 (Electronic Credentials, Not Identity Proofed): 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.

II PRICE PROPOSAL FACTOR : See SCP-FSS-001 and SCP-FSS-004