CI-FSS-152-N ADDITIONAL EVALUATION FACTORS FOR NEW OFFERORS UNDER SCHEDULE 70 (APR 2019)

(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 (HACS), 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, SIN 132-40 Cloud and Cloud-Related IT Professional Services only.

(A) Provide a description of the offeror's experience in the professional information technology services offered under SIN 132-20, SIN 132-40 Cloud-Related IT Professional Services only, SIN 132-41, SIN 132-45 Highly Adaptive Cybersecurity Services (HACS), 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 132-40 Cloud-Related IT Professional Services only, SIN 132-41, SIN 132-45, 132-51, 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 (HACS) 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)). The Self-Attestation form is available at "gsa.gov/hacs".

An offeror may only be awarded SIN 132-45, Highly Adaptive Cybersecurity Services 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 5 subcategories. The base HACS 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 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 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 passed under this evaluation factor shall be failed and shall be ineligible to re-submit under the SIN to participate in this evaluation factor for a period of six (6) months following the date of failure.

(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 Highly Adaptive Cybersecurity Services oral technical evaluation, so long as they provide in the modification package to the GSA Contracting Officer a Service Self-Attestation acknowledging their ability to perform Security Architecture Review (SAR) and Systems Security Engineering (SSE) services in their entirety. The Self-Attestation form is available at "gsa.gov/hacs".

(iii) ORAL TECHNICAL EVALUATION PROCEDURES

The offeror will be evaluated on their knowledge of the proposed services. The oral technical evaluation will require the offeror to respond to a specific scenario and general questions to assess the offeror's expertise. The competencies, criteria and evaluation minimums for the questions are below:

All new offerors and modifications must participate in and PASS the HACS Oral Technical Evaluation. The Oral Technical Evaluation will include, at a minimum, questions on Risk and Vulnerability Assessment (RVA), Security Architecture Review (SAR), Systems Security Engineering (SSE), and Penetration Testing. At the time of submission, all new offerors and modifications can also elect to be cataloged in one or both of the additional subcategories of Cyber Hunt or Incident Response (IR). Should this election be taken, additional questions related to these subcategories will be included in their HACS evaluation and these additional subcategory topics must be passed as well.

(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 offeror has the requisite experience and expertise to perform tasks expected to be performed within the scope of the SIN. The oral technical proposal will be evaluated and rated on a pass/fail basis. The rating definitions provided below will be used for the evaluation of the offeror's responses to questions during the oral evaluation.

TECHNICAL RATINGS

Rating	Definition
Pass	The proposal meets the minimum requirements of the solicitation.
Fail	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.

(7) FACTOR 7: Cloud Computing Services Qualification Requirements for SIN 132-40 (Cloud Computing Products i.e., IAAS, SAAS, PAAS). See SCP-FSS-004.

A. FACTOR - Cloud Computing Services Adherence to Essential Cloud Characteristics

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

- On-demand self-service
- Broad network access
- Resource Pooling
- Rapid Elasticity
- Measured Service

Refer to the ‘Guidance for Contractors’ section of the Terms & Conditions for Cloud and Cloud-Related IT Professional Services SIN for guidance on meeting the NIST characteristics. For the purposes of the Cloud Computing Services SIN, meeting the NIST essential characteristics is concerned primarily with whether the underlying capability of the commercial service is available, whether or not an Ordering Activity actually requests or implements the capability

B. FACTOR – Cloud Computing Services Deployment Model

For each cloud service submitted, provide a written description of how the proposed service meets the NIST definition of a particular deployment model (Public, Private, Community, or Hybrid), within a one half (1/2) page limitation for each designated deployment model of each cloud service submitted. Multiple deployment model selection is permitted, but at least one model must be indicated. Refer to the ‘Guidance for Contractors’ section of the Terms & Conditions for the Cloud Computing Services SIN for guidance on identifying the appropriate deployment model according to the NIST service model definitions.

C. FACTOR - Cloud Computing Services Service Model

For each cloud computing service proposed to be categorized under a specific sub-category (IaaS, PaaS or SaaS), provide a written description of how the proposed service meets the NIST definition of that service model, within a half (1/2) page limitation for each cloud service submitted. Refer to the ‘Guidance for Contractors’

section of the Terms & Conditions for the Cloud Computing Services SIN for guidance on categorizing the service into a sub-category according to the NIST service model definitions.

Note that it is not mandatory to select a sub-category, and therefore this factor for evaluation applies ONLY to cloud services proposed to fall under a specific sub-category. If no sub-category is selected, this factor does not need to be addressed. The two other factors ('Adherence to Essential Cloud Characteristics' and 'Cloud Computing Services Deployment Model') apply to all cloud services.