----- 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 132-45A Penetration Testing, SIN 132-45B Incident Response, SIN 132-45C Cyber Hunt, SIN 132-45D Risk and Vulnerability Assessment, SIN 132-51 IT Professional Services, 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, SIN 132-45A, SIN 132-45B, SIN 132-45C, SIN 132-45D, SIN 132-51

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 132-45A, SIN 132-45B, SIN 132-45C, SIN 132-45D, 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 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. Offerors proposing services under SIN 132-45A Penetration Testing, SIN 132-45B Incident Response, SIN 132-45C Cyber Hunt, and/or SIN 132-45D Risk and Vulnerability Assessments additional requirements are:

ORAL TECHNICAL EVALUATION OVERVIEW: 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 SIN as set forth in this solicitation.

Offeror/Contractor shall review Factor 5 Oral Technical Evaluation Criteria in SCP-FSS-004 section (d)(II)(5)(iii) to this solicitation for details on the knowledge

areas to be assessed in the evaluation and the criteria for a ‘Acceptable’ or ‘Unacceptable’ rating under this factor.

(i) ORAL TECHNICAL EVALUATION CONSTRAINTS: The offeror shall identify up to five key personnel, by name and association with the offeror, who will field questions during the oral technical evaluation. After opening remarks by the TEB, the offeror will respond to a series of questions and scenarios in 40 minutes per SIN. The evaluation will be stopped precisely after 40 minutes. The total evaluation session is expected to up to three (3) hours, depending on the number of SINs 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.

(ii) 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 make accommodations for vendors to participate in the oral evaluations virtually, if they are unable to participate in-person.

(iii) 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.

(iv) RESUBMISSION RESTRICTIONS FOR UNSUCCESSFUL VENDORS UNDER THIS EVALUATION FACTOR: Offeror, whom the TEB has found to have not met the “acceptable” criteria under this evaluation factor shall be given one (1) opportunity to provide clarifications to the TEB. The offeror will have 24 hours from the time of the notice from the TEB to provide clarifications. Offerors, who have provided clarifications and still have not met the “acceptable” criteria, shall be rejected and shall be ineligible to re-submit proposals to participate in the SIN for which they were rejected for a period of six (6) months following the date of rejection.

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

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

----- 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 132-45A Penetration Testing, SIN 132-45B Incident Response, SIN 132-45C Cyber Hunt, SIN 132-45D Risk and Vulnerability Assessment, 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 132-45A Penetration Testing, SIN 132-45B Incident Response, SIN 132-45C Cyber Hunt, and/or SIN 132-45D Risk and Vulnerability Assessments.

(A) 132 – 45 Penetration Testing

Expected tasks within the scope of this SIN include but are not limited to:

- Conducting and/or supporting authorized penetration testing on enterprise network assets
- Analyzing site/enterprise Computer Network Defense policies and configurations and evaluate compliance with regulations and enterprise directives
- Assisting with the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems, and processes)

(B) 132-45B Incident Response

Expected tasks within the scope of this SIN include but are not limited to:

- Collect intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise
- Perform command and control functions in response to incidents
- Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation

(C) 132-45C Cyber Hunt

Expected tasks within the scope of this SIN include but are not limited to:

- Collecting intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise

- Coordinating with and provide expert technical support to enterprise-wide Computer Network Defense technicians to resolve Computer Network Defense incidents

- Correlating incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation

(D) 132-45D Risk and Vulnerability Assessments (RVA)

At a minimum offerors who would like to be considered for this SIN must offer the following services:

- Network Mapping - consists of identifying assets on an agreed upon IP address space or network range(s).

- Vulnerability Scanning - comprehensively identifies IT vulnerabilities associated with agency systems that are potentially exploitable by attackers.

- Phishing Assessment - includes activities to evaluate the level of awareness of the agency workforce with regard to digital form of social engineering that uses authentic looking, but bogus, emails request information from users or direct them to a fake Website that requests information. Phishing assessments can include scanning, testing, or both and can be conducted as a one- time event or as part of a larger campaign to be conducted over several months.

- Wireless Assessment - includes wireless access point (WAP) detection, penetration testing or both and is performed while onsite at a customer's facility.

- Web Application Assessment - includes scanning, testing or both of outward facing web applications for defects in Web service implementation may lead to exploitable vulnerabilities. Provide report on how to implement Web services securely and that traditional network security tools and techniques are used to limit access to the Web Service to only those networks and systems that should have legitimate access.

- Operating System Security Assessment (OSSA) - assesses the configuration of select host operating systems (OS) against standardized configuration baselines.

- Database Assessment - assesses the configuration of selected databases against configuration baselines in order to identify potential misconfigurations and/or database vulnerabilities.

- SIN 132-45A - Penetration Testing - conducting and/or supporting authorized Penetration Testing on enterprise network assets.

(ii) ORAL TECHNICAL EVALUATION OVERVIEW: 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 SIN as set forth in this solicitation.

Offeror/Contractor shall review Factor 5 Oral Technical Evaluation Procedure in SCP-FSS-004 section (d)(II)(5)(iii) to this solicitation for details on the knowledge areas to be assessed in the evaluation and the criteria for a 'Acceptable' or 'Unacceptable' rating under this factor.

(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. After opening remarks by the TEB, the offeror will respond to a series of questions and scenarios in 40 minutes per SIN. The evaluation will be stopped precisely after 40 minutes. The total evaluation session is expected to up to three (3) hours, depending on the number of SINs 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 make accommodations for vendors to participate in the oral evaluations virtually, if they are unable to participate in-person.

(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: Offeror, whom the TEB has found to have not met the "acceptable" criteria under this evaluation factor shall be given one (1) opportunity to provide clarifications to the TEB. The offeror will have 24 hours from the time of the notice from the TEB to provide clarifications. Offerors, who have provided clarifications and still have not met the "acceptable" criteria, shall be rejected and shall be ineligible to re-submit proposals to participate in the SIN for which they were rejected for a period of six (6) months following the date of rejection.

(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:

(A) SIN 132-45 A - Penetration Test Evaluation Overview - As part of the oral evaluation, the offeror will respond to a scenario to demonstrate their level of competency as it relates to the performance of penetration activities which typically include reconnaissance, scanning and enumeration, exploitation, and pivoting.

i Competency: Reconnaissance (Passive & Active)

(1) Criteria: Passive Reconnaissance Minimums in responding to the scenario:

(a) The offeror must state at least three Tactics, Techniques, & Procedures (TTPs) used for conducting passive reconnaissance.

(2) Criteria: Active Reconnaissance Minimums in responding to the scenario:

(a) The offeror must state at least two Tactics, Techniques, & Procedures (TTPs) used for conducting active reconnaissance.

ii Competency: Scanning and Enumeration

(1) Criteria: Scanning Methodology Minimums in responding to the scenario:

(a) The offeror must clearly explain in detail their overall scanning methodology for detecting live systems and identifying existing vulnerabilities to be exploited. The offeror must demonstrate they have a structured and ordered approach.

(2) Criteria: Identify Preferred Tools Minimums in responding to the scenario:

The offeror should speak to a few tools used in scanning and enumeration of systems and vulnerabilities. The offeror must identify at least three (3) tools.

iii Competency: Exploitation

(1) Criteria: Delivery Installation/Modification, Execution of Attack Minimums in responding to the scenario:

(a) The offeror must clearly explain some of the techniques used to exploit vulnerabilities. The offeror must identify at least four
(4) techniques.

(2) Criteria: Methods for bypassing F/W, AV, IDS/ NIDS, IPS, etc. Minimums in responding to the scenario:

(a) The offeror must clearly explain some of the techniques used to bypass defense-in-depth technologies. The offeror must identify at least three (3) techniques.

(3) Criteria: Offeror's Capability to develop their own custom exploits Minimums in responding to the scenario:

(a) The offeror must clearly explain some of the programming languages used to develop custom exploits. The offeror must identify at least two (2) programming languages.

(4) Criteria: Offeror Preferred Tools Minimums in responding to the scenario:

(a) The offeror should speak to a few tools used when exploiting vulnerabilities. The offeror should identify at least four (4) tools.

iv Competency: Pivoting

(1) Criteria: Further your access Minimums in responding to the scenario:

(a) The offeror should speak to a few techniques and procedures used when pivoting to further access. The offeror must identify at least three (3) techniques and procedures.

(2) Criteria: Methods used to establish and maintain command and control mechanisms e.g. advanced persistent testing (APT) Minimums in responding to the scenario:

(a) The offeror should speak to a few techniques and procedures used when pivoting to main access and control of the victim's system. The offeror must identify at least two (2) techniques and procedures.

(3) Criteria: Offeror Preferred Tools Minimums in responding to the

scenario:

(a) The offeror should speak to a few tools used when pivoting to maintain and escalate control. The offeror may identify at least three (3) tools.

(B) SIN 132-45 B - Incident Response Evaluation Overview - As part of the oral evaluation, the offeror will respond to a scenario to demonstrate their level of competency as it relates to the performance of incident

response activities which typically include preparation, identification, containment, eradication, recovery, and lessons learned.

i Competency: Preparation

(1) Criteria: Preparation Minimums in responding to the scenario:

(a) The offeror must state at least two (2) communication and coordination mechanisms that should be implemented.

ii Competency: Detection and Analysis

(1) Criteria: Detection & Analysis Minimums in responding to the scenario:

(a) The offeror must state at least two (2) items leveraged in the detection of an indicator of compromise.

iii Criteria: Incident Prioritization Minimums in responding to the scenario:

(1) The offeror must state at least two (2) approaches for analyzing and prioritizing incidents.

iv Competency: Containment and Remediation

(1) Criteria: Containment Minimums in responding to the scenario:

(a) The offeror must clearly explain appropriate containment methods. The offeror must identify at least three (3) methods.

v Criteria: Eradication Minimums in responding to the scenario:

(1) The offeror must clearly explain some of the methods used to eradicate an incident. The offeror must identify at least two (2) eradication methods.

vi Criteria: Recovery/Remediation Minimums in responding to the scenario:

(1) The offeror must clearly explain some remediation elements to restore normal operations. The offeror must identify at least three (3) remediation elements.

vii Competency: Post-Incident Support

(1) Criteria: Follow-Up Actions Minimums in responding to the scenario:

(a) The offeror should speak to types of post-incident activities that are performed. The offeror must identify at least two (2) activities.

viii Criteria: Lessons Learned Minimums in responding to the scenario:

(1) The offeror should speak to a few lessons learned discussion questions during a post-incident review. The offeror must identify at least two (2) lessons learned discussion points.

(C) SIN 132-45 C - Cyber Hunt Evaluation Overview - As part of the oral evaluation, the offeror will respond to a scenario to demonstrate their level of competency as it relates to the performance of Cyber Hunt activities which typically include, Creating a Hypothesis, Investigating via Tools & Techniques, Uncovering New Patterns and Tactics, Techniques, & Procedures (TTPs) and Informing & Enriching Analytics.

i Competency: Hypothesis Creation/ Generation

(1) Criteria: Hypothesis Creation/ Generation Minimums in responding to the scenario:

(a) The offeror must clearly explain in detail their process for developing hypotheses. The Hypothesis Creation/Generation Hunting Maturity (HM) Levels will be used to assess the offerors HM level. The offeror must exceed the “HMO Initial” level.

ii Competency: Tools & Techniques for Hypothesis Testing

(1) Criteria: Tools & Techniques for Hypothesis Testing Minimums in responding to the scenario:

(a) The offeror must clearly explain in detail how they utilize their tools and techniques to address their hypotheses. The Tools & Techniques for Hypothesis Testing Hunting Maturity (HM) Levels will be used to assess the offeror's HM level. The offeror must exceed the “HMO Initial” level.

iii Competency: Pattern and Tactics, Techniques, & Procedures (TTPs) Detection

(1) Criteria: Pattern and Tactics, Techniques, & Procedures (TTPs) Detection Minimums in responding to the scenario:

(a) The offeror must clearly explain in detail how they identify IoC patterns and Tactics, Techniques, & Procedures (TTPs) that were discovered in hypotheses testing. The Pattern & Tactics, Techniques and Procedures (TTPs) Detection Hunting Maturity (HM) Levels will be used to assess the offeror's HM level. The offeror must exceed the "HMO Initial" level.

iv Competency: Analytics Automation

(1) Criteria: Analytics Automation Minimums in responding to the scenario:

(a) The offeror must clearly explain in detail techniques for developing analytics automation processes and procedures. The Analytics Automation Hunting Maturity (HM) Levels will be used to assess the offeror's HM level. The offeror must exceed the "HMO Initial" level.

(D) SIN 132-45 D - Risk and Vulnerability Assessment Evaluation Overview - As part of the oral evaluation, the offeror will respond to a scenario to demonstrate their level of competency as it relates to the performance of the RVA process which includes; Pre-Assessment/Planning Phase, Testing/Assessment Phase and
Post-Assessment Phase.

i Competency: Pre-Assessment/Planning Phase

(1) Criteria: Preliminary Activities Minimums in responding to the scenario:

(a) The offeror must clearly explain in detail their overall preliminary activities prior to conducting RVA. The offeror must demonstrate they have a structured and ordered approach.

ii Competency: Testing/Assessment Phase

(1) Criteria: Assessment Activities Minimums in responding to the scenario:

(a) The offeror must clearly explain in detail their overall activities for conducting RVA. The offeror must demonstrate that they have a structured and ordered approach.

(2) Criteria: RVA Service Catalog Minimums in responding to the scenario:

(a) The offeror must clearly explain in detail the specific services that they provide for conducting RVA. The offeror must provide all of the services listed below:

- Network Mapping
- Vulnerability Scans
- Penetration Testing
- Phishing Assessment
- Wireless Assessment
- Web Application Assessment
- Operating System Security Assessment
- Database Assessment

(3) Criteria: Assessment Tools Minimums in responding to the scenario:

(a) The offeror must clearly explain in detail the specific assessment tools that they utilize for conducting RVA.

iii Competency: Post Assessment Phase

(1) Criteria: Final Report Minimums in responding to the scenario:

(a) The offeror must clearly explain in detail the final reporting process that they utilize for conducting RVA.

iv 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

(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 these SINs. Each 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 clearly meets the minimum requirements of the solicitation.
Unacceptable	The proposal does not clearly 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	SCA Equivalent Code Title	WD Number

Category		
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)."