Request for Proposals (RFP) No.	RFP-24-10020-03
Issue Date	August 20, 2024
Project Title	USAID Ukraine Monitoring and Learning Support Contract
Amendment Date	n/a
Issuing Office and Email Address for Submission of Proposals	EnCompass LLC
Instructions for Proposal Submission	Proposals must be submitted via email. The maximum size per email is 22MB
Deadline for Receipt of Questions from Offerors	Tuesday, August 27, 2024 at 5 p.m. EST
EnCompass Responses to Questions to Offerors	Friday, August 30, 2024, at 5 p.m. EST
Deadline for Receipt of Proposals	Friday, September 20, 2024, at 5 p.m. EST
Point of Contact	mrichardson@encompassworld.com To receive direct notification of any RFP amendments or other announcements related to this RFP, potential bidders may register their interest by sending an email to mrichardson@encompassworld.com with the subject: RFP-10020-24-03 Security Services
Award Type	EnCompass intends to issue a Time and Materials (T&M) agreement which may be incrementally funded. USAID's approval of consent to subcontract is required.
Estimated Date of Award	October 24, 2024
Ceiling (if applicable)	TBD
Period of performance	October 24, 2024 until March 1, 2027

1 INTRODUCTION AND SCOPE OF WORK

1.1 Introduction

EnCompass, the prime contractor of the United States Agency for International Development (USAID) Ukraine Monitoring and Learning Support Contract (UMLS) invites Offerors to submit proposals to supply and deliver security services which are detailed in the following Scope of Work. UMLS assists the Mission for Ukraine and Belarus (USAID/Ukraine) in addressing its overall monitoring, evaluation, and collaborating, learning, and adapting (CLA) needs during the implementation of its Country Development Cooperation Strategy (CDCS) and beyond.

The Offeror will support the EnCompass UMLS team in overall security support for the project office and staff located in Kyiv, Ukraine, and for temporary visitors to ensure proper duty of care. UMLS currently has approximately 10 staff located in Kyiv, including 3 expatriate staff. EnCompass needs to establish a security approach and infrastructure that allows for effective and safe delivery of the UMLS contract.

EnCompass seeks qualified, experienced, and reputable security providers to support EnCompass in its delivery of UMLS objectives, allowing UMLS personnel to work safely and effectively within Ukraine, and reduce the risk for staff and the organization. EnCompass invites Offerors to submit proposals to supply and deliver security support services, which are detailed in section 1.3, Scope of Work, of this Request For Proposal (RFP).

1.2 Type of Award Anticipated

EnCompass anticipates awarding a T&M agreement. This agreement type is subject to change during negotiations.

Time and Materials: The purchase of labor and materials (non-labor), with labor rates being inclusive of all costs associated with that labor cost. The anticipated T&M agreement will have an overall ceiling; however, it will be managed based on the on-demand services detailed in section 1.3, Scope of Work.

1.3 Scope of Work

The work of the subcontractor will focus on providing ongoing security services and maintaining overall responsibility for security related to UMLS staff, visitors, and activities, including but not limited to the below responsibilities. Please propose the tasks and level of effort for a 28-month period of performance. The budget table in section 3.16 includes a “plug figure” that is made to cover other direct costs (ODC). This figure can be adjusted upon submission in line with the Offeror’s proposal.

The subcontractor will be responsible for the implementation of the UMLS Security Plan including:

Reporting

- Update and maintain the **UMLS Security Plan** and provide guidance as needed for inputs on security-related contract deliverables.
- Conduct periodic project **Security Audits** (once per quarter) to ensure compliance with security policies, procedures, and standards, including reviews of adherence to security guidance and procedures during emergencies, TDYs, etc. EnCompass will provide guidance on the format and requirements for the Security Audit.
- **Location Security Assessments** of expanded or new office and living quarters for USN and TCN staff.
- Provide **Local Security Alerts** in signal channel for various audiences inclusive of threat alerts and hibernation guidance. Contents and organization of alerts may be adjusted based on input/feedback from Chief of Party (COP), Crisis Management Team (CMT), or UMLS Corporate Officer.
- Provision of a **Weekly Security Report**, 7 pages maximum, containing summary information on real or anticipated changes in the security profile of Kyiv and other parts of the country. Contents and organization of the report may be adjusted based on input/feedback from Chief of Party, CMT, and/or UMLS Corporate Officer.
- Development of a detailed and **Scenario-Based Hibernation and Evacuation Plan (CHEP)** for USN/TCN staff. This plan should be updated regularly, with clear triggers in place, appropriate actions to be taken, and alternate plans in case of varying contingencies. This Plan is due 30 days from subcontract award and should include plans for all current UMLS USN/TCN staff.
- Ad hoc reporting to the CMT, as requested and appropriate.

Training Services

- Conduct training for UMLS staff working from the office in Kyiv, and other parts of the country as appropriate, on the UMLS Security Plan and others, described below.
- Development and implementation of a staff training program on security protocols in the office and commuting to the office.
- Security training for all UMLS staff, staff on short term technical assignments (STTA), expats and local. This should include protection, hibernation, and emergency medical training and may be requested on demand. It is estimated these trainings will be held at least twice per year.

Advisory Services

- Advise the EnCompass project team on how to comply with security requests from USAID, including the USAID Partner Security Liaison Office (PLSO).
  - Provide guidance on procurement of security related equipment, as requested.
- Review and approve second and third tier subcontractor/vendor Security Plans (partners conducting MEL and TPM services throughout Ukraine).
  - Provide on demand crisis management support on an as needed basis.

- Participate in USAID and other security-related meetings organized in Ukraine or elsewhere (virtual). Provide a report out to the UMLS team on key takeaways and any recommended adjustments to the UMLS Security Plan.
- Manage and oversee UMLS Security Signal Channels, documenting participants, purpose, content, etc.

Travel/Evacuation Support Services

- Development of Journey Management Plans (JMP) for staff traveling to Ukraine, including STTA to High and Extreme risk locations as requested by UMLS inclusive of location assessments.
- Conduct pre departure briefings, track movements in route to and from destinations, and brief temporary duty assignments when they first arrive in Kyiv on UMLS procedures.
- Coordination with evacuation provider, International SOS, as needed. Emergency coordination will be conducted in conjunction with the CMT.
- Provide on demand travel location reviews for subcontractors/vendors who will be traveling to various oblasts throughout Ukraine. For this type of review, all UMLS will ask from the subcontractor is a 'green' or 'red' light for travel.

Security Staffing

- Provision of a senior in-country (Kyiv-based) security presence by a part-time USN/TCN security manager.
- Provision of a mid-level security manager to support threat monitoring.
- Alignment of all staffing with labor categories, rates, and experience requirements.

Coordination

- Meet regularly with COP and in country Security Focal Point to discuss ongoing security services and anticipated needs (frequency, location, and agenda to be set by COP)
- Meet semi-regularly with the EnCompass Corporate Officer and CMT to review recent audits, scenario changes, and upcoming/anticipated needs.
- Meet as needed with UMLS home office management team related to implementation of the subcontractor management plan.

2 PRIME AWARD FLOWDOWNS and SPECIAL REQUIREMENTS

The terms presented below will be included in any agreement issued as a result of successful Offers in response to this RFP. By submitting a proposal in response to this RFP, Offerors acknowledge their review and acceptance of the following requirements.

2.1 Prohibited Technology

Offerors MUST NOT provide any goods and/or services that utilize telecommunications and video surveillance products from the following companies: Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company, or any subsidiary or affiliate thereof, in compliance with FAR 52.204-25.

2.2 Source and Nationality

The authorized geographic code authorizes EnCompass to procure goods and services only from the following countries. A waiver to these requirements may be sought by EnCompass if the Offeror selected is registered in a country outside of Geographic Code 937 and 110.

Geographic Code 110: Goods and services from the independent states of the former Soviet Union.

Geographic Code 937: Goods and services from the United States, the cooperating country, and "Developing Countries" other than "Advanced Developing Countries" excluding prohibited countries. A list of the "Developing Countries" as well as "Advanced Developing Countries" can be found at:

https://www.usaid.gov/ads/policy/300/310maa and

https://2012-2017.usaid.gov/sites/default/files/documents/1876/310mab.pdf respectively.

The source and nationality of goods and services must be verified by EnCompass to ensure that procurement of any goods or services from prohibited countries listed by the Office of Foreign

Assets Control (OFAC) as sanctioned countries is not made. OFAC sanctioned countries may be searched within the System for Award Management (SAM) at www.SAM.gov. The current list of countries under comprehensive sanctions include: Cuba, Iran, North Korea, Sudan, and Syria. Goods may not transit through or be assembled in comprehensive sanctioned origin or nationality countries nor can the vendor be owned or controlled by a prohibited country. EnCompass is prohibited from facilitating any transaction by a third party if that transaction would be prohibited if performed by EnCompass.

By submitting a proposal in response to this RFP, Offerors confirm that they are not violating the Source and Nationality requirements of the goods or services being offered and that the goods and services comply with the exclusions for prohibited countries outlined above.

2.3 Security Clause

The subcontractor acknowledges and accepts the security conditions of the regions and zones where the activities will take place. The subcontractor accepts that there will be no compensation in any case where its personnel or assets are affected by the security conditions during any travel to the regions where the activities are being implemented.

2.4 Logistics Support

The subcontractor shall be responsible for furnishing all travel and logistical support where the work will be performed.

2.5 Executive Order on Terrorism Financing (Feb 2002)

The subcontractor is reminded that U.S. Executive Orders and U.S. law prohibits transactions with, and the provision of resources and support to, individuals and organizations associated with terrorism. It is the responsibility of the contractor/recipient to ensure compliance with these Executive Orders and laws. This provision must be included in all subcontracts/subaward issued under this contract/agreement. Recipients may not engage with, or provide resources or support to, individuals and organizations associated with terrorism. No support or resources may be provided to individuals or entities that appear on the Specially Designated Nationals and Blocked persons List maintained by the US Treasury (online at www.SAM.gov) or the United Nations Security Designation List (online at:

http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml).

This provision must be included in all subcontracts/sub awards issued under this Contract.

2.6 DOSAR 652.243-70 Notices (Aug 1999)

Any notice or request relating to this contract given by either party to the other shall be in writing. Said notice or request shall be mailed or delivered by hand to the other party at the address provided in the schedule of the contract. EnCompass must make all modifications to the contract in writing.

2.7 Subcontracting

Prior written approval by the Encompass Contract Representative is required to engage lower-tier subcontractors. Costs for lower-tier subcontracts that do not have prior written approval in accordance with this Agreement will not be reimbursed. Inclusion of lower-tier subcontractor costs in the Subcontractor budget or proposal does not constitute a request or approval. Note that this restriction does not apply to commercial vendors.

2.8 Termination of Subcontract

Subcontractors shall remain in effect from the date hereof and shall terminate upon the earliest of the following:

a) For Cause: This subcontract may be terminated for cause at any time, in whole or in part, by Encompass upon written notice. If the Subcontractor fails to comply with contract requirements, then the subcontractor will be given 30 days to remedy the non-compliance before termination is considered.

b) For Convenience: This subcontract may be terminated for convenience by written notice, in whole or in part, by EnCompass or if termination is directed by USAID. If this subcontract is terminated, the termination conditions, including the effective date and, in the case of partial termination, the portion to be terminated, will be provided in the notice.

c) Termination Procedures: Upon receipt of, and in accordance with, a termination notice as specified in either paragraph above, Subcontractor will take immediate action to stop work and minimize all expenditures and obligations financed by this subcontract. Subcontractor will also cancel unliquidated obligations whenever possible. Encompass agrees to reimburse Subcontractor for work completed up to the date of termination on behalf of Encompass.

d) Termination Notice: The Prime Contractor will give thirty (30) business days' notice where possible prior to termination date.

2.9 Confidential Information

The Subcontractor agrees, in the performance of this subcontract, to keep the information furnished by EnCompass or its client, or acquired/developed by the Subcontractor in performance of the subcontract and designated by EnCompass and its client, in the strictest confidence. The Subcontractor also agrees not to publish or otherwise divulge such information, in whole or in part, in any manner or form, nor to authorize or permit others to do so, taking such reasonable measures as are necessary to restrict access to such information while in the Subcontractor's possession, to those employees needing such information to perform the work described herein, i.e., on a “need-to-know” basis. The Subcontractor agrees to immediately notify the EnCompass Contracts Representative in writing in the event that the Subcontractor determines or has reason to suspect a breach of this requirement has occurred.

All Subcontractor staff working on any of the described tasks may, at the request of EnCompass on behalf of its client, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of information and documents of the EnCompass Client. The Contractor (EnCompass) shall insert the substance of this special contract requirement, including this paragraph (c), in all subcontracts when requiring a restriction on the release of information developed or obtained in connection with performance of the contract.

2.10 General Terms and Conditions

Notices. The individuals identified on the cover page of this Agreement are authorized by each party to receive notices.

a) Relationship. For the purpose of the subcontract, Encompass will be the Prime Contractor to the party identified in this Subcontract Agreement. Nothing in this Agreement shall be construed to create a joint venture or partnership between the parties, and nothing in this Agreement shall be deemed to create an

agency relationship between the Parties or authorize a Party to commit or bind the other Party in any way whatsoever.

b) Prime Contractor Client. This agreement is issued under a prime contract with Encompass LLC and shall not be construed in any way to create a contractual relationship between the Subcontractor and USAID. The Subcontractor shall not appeal directly to USAID without the written consent/ concurrence of the Encompass Contract Representative.

c) Consideration. The rights and obligations of the parties to this subcontract shall be subject to and governed by this subcontract. All applicable clauses under this award shall be supported by the Subcontractor's certified Representations and Certifications.

d) Entire Agreement. This Agreement constitutes the entire agreement between the Parties hereto concerning the subject matter hereof and supersedes any prior or contemporaneous agreements and understandings concerning the subject matter hereof.

e) No Assignment. Neither Party may assign or transfer or attempt to assign or transfer this Agreement to any person or entity without the prior written consent of the other Party.

2.11 Ownership

All reports, presentations and other work products related hereto produced by a subcontractor will be considered data, subject to the provisions of far 52.227-14, "Rights in Data - General, Alternate IV." Encompass, on behalf of its funder USAID, shall have the irrevocable, fully paid up right to use, release to others, reproduce, distribute and publish such data.

2.12 Stop Work Order

Encompass may issue a written notice to stop all or any part of the work called for by a subcontract. Upon receipt of the notice, the subcontractor will stop all work and take all reasonable steps to minimize incurring allocable costs. Encompass shall either cancel the work order by written notice, or terminate the subcontract in accordance with the Termination clause of this agreement. Performance of work by the Subcontractor shall resume upon cancellation or expiration of any stop work order.

2.13 Combating Trafficking in Persons

Under this Federally-funded agreement, trafficking in persons is prohibited, including any trafficking-related activities. The provisions set forth in FAR 52.222-50, Combating Trafficking in Persons are applicable to the Subcontractor, as well as FAR 52.222-56, Certification Regarding Trafficking in Persons Compliance Plan. Information regarding trafficking in persons is found at the U.S. Department of State's Office to Monitor and Combat Trafficking in Persons website:

http://www.state.gov/j/tip/.

2.14 Standard of Conduct

The Subcontractor must be responsible for maintaining satisfactory standards of employee competency, conduct appearance and integrity, and must be responsible for taking such disciplinary action with respect to employees as may be necessary while implementing work. The Subcontractor is also responsible for ensuring that his/her employees do not use Government resources except as authorized by the Government.

2.15 Prohibition of Assistance to Drug Traffickers

USAID reserves the right to terminate the Subcontract, to demand a refund or take other appropriate measures if the Subcontractor is found to have been convicted of a narcotics offense or to have been engaged in drug trafficking as defined in 22 CFR Part 140.

2.16 Reporting Waste, Fraud, Abuse, and Theft

The Subcontractor shall notify the EnCompass Contracting Representative and the Chief of Party of any instances of suspected waste, fraud, abuse, loss, or theft of Subcontractor or Government-furnished property by employees or Subcontractors.

2.17 Foreign Corrupt Practices Act

The Subcontractor shall comply fully with the anti-bribery provisions of the U.S. Foreign Corrupt Practices Act, as amended ("FCPA"), as well as the a) UN Conventional against Corruption (UNICAC), b) OECD Convention on the Bribery of Foreign Public Officials (OECD Convention); and c) any other applicable local anticorruption laws, rules, and regulations if any part of this Agreement, or any Subcontract issued hereunder, will be performed outside of the United States of America.

The Subcontractor acknowledges and agrees that it is unlawful for the contractor and/or any officer, director, employee or agent of the contractor to make any kind of offer, payment, promise to pay, or authorization of the payment of any money, or offer, gift, promise to give, or authorization of the giving of anything of value to:

- A foreign official (or foreign political party) for purposes of either influencing any act or decision of such foreign official in his official capacity.
- A person, that could offer, give or promise monies or something of value, either directly or indirectly, to any foreign official (or foreign political party), or to any candidate for foreign political office.

Under this Agreement, a "foreign official" is any appointed, elected, or honorary official or employee of a foreign government or a public international organization, or any person acting in an official capacity for or on behalf of any such government or department, agency, or instrumentality, or for or on behalf of any such public international organization (e.g., the World Bank, UN, DFID, or WHO).

For purposes of this Article, the "government" includes any agency, department, embassy, or other governmental entity, and any company or other entity owned or controlled by the government.

The Subcontractor agrees not to interact with any government official, political party or public international organization on behalf of the Prime Contractor, without prior written authorization, outside of contractor's performance of the Statement of Work.

2.18 Code of Ethics

Encompass has established high ethical standards for its employees, subcontractors, independent contractors and vendors. Encompass adheres to its Code of Ethics and all U.S. and non-U.S. laws and regulations. Under the terms of this Agreement, Subcontractor is required to maintain a Code of Business Ethics and Conduct in compliance with FAR 52.203-13. Subcontractor is required to report any violation of the Subcontractor's Code of Business Ethics and Conduct committed by an employee(s) of either party, or anyone affiliated with the Subcontractor, to Encompass.

2.19 Fly America Act

The Offeror must comply with Fly America Act restrictions for all international travel under this award.

1. The recipient must use U.S. Flag Air Carriers for all international air transportation (including personal effects) funded by this award pursuant to the Fly America Act and its implementing regulations to the extent service by such carriers is available.
2. In the event that the recipient selects a carrier other than a U.S. Flag Air Carrier for international air transportation, in order for the costs of such international air transportation to be allowable, the recipient must document such transportation in accordance with this provision and maintain such documentation pursuant to the Standard Provision, "Accounting, Audit and Records." The documentation must use one of the following reasons or other exception under the Fly America Act:
   A. The recipient uses a European Union (EU) flag air carrier, which is an airline operating from an EU country that has signed the US-EU "Open Skies" agreement

(http://www.state.gov/e/eb/rls/othr/ata/i/ic/170684.htm)

   B. Travel to or from one of the following countries on an airline of that country when no city pair fare is in effect for that leg (see http://apps.fas.gsa.gov/citypairs/search/):
      - Australia on an Australian airline,
      - Switzerland on a Swiss airline, or
      - Japan on a Japanese airline;
   C. Only for a particular leg of a route on which no US Flag Air Carrier provides service on that route;
   D. For a trip of 3 hours or less, the use of a US Flag Air Carrier at least doubles the travel time;
   E. If the US Flag Air Carrier offers direct service, use of the US Flag Air Carrier would increase the travel time by more than 24 hours; or
   F. If the US Flag Air Carrier does not offer direct service,
      - Use of the US Flag Air Carrier increases the number of aircraft changes by 2 or more,
      - Use of the US Flag Air Carrier extends travel time by 6 hours or more, or

- Use of the US Flag Air Carrier requires a layover at an overseas interchange of 4 hours or more.

Definitions

The terms used in this provision have the following meanings:

1. “Travel costs’’ means expenses for transportation, lodging, subsistence (meals and incidentals), and related expenses incurred by employees who are on travel status on official business of the recipient for any travel outside the country in which the organization is located. “Travel costs” do not include expenses incurred by employees who are not on official business of the recipient, such as rest and recuperation (R&R) travel offered as part of an employee’s benefits package that are consistent with the recipient’s personnel and travel policies and procedures.
2. “International air transportation" means international air travel by individuals (and their personal effects) or transportation of cargo by air between a place in the United States and a place outside thereof, or between two places both of which are outside the United States.
3. "U.S. Flag Air Carrier" means an air carrier on the list issued by the U.S. Department of Transportation at http://ostpxweb.dot.gov/aviation/certific/certlist.htm. U.S. Flag Air Carrier service also includes service provided under a code share agreement with another air carrier when the ticket, or documentation for an electronic ticket, identifies the U.S. flag air carrier’s designator code and flight number.
- For this provision, the term “United States” includes the fifty states, Commonwealth of Puerto Rico, possessions of the United States, and the District of Columbia.

2.20 Insurance

Offeror certifies that it shall maintain the following insurance in at least the minimum amounts required by law. The Subcontractor shall require its lower tier subcontractors to maintain insurance at, or in excess of, the limits stated below:

1. Workers’ Compensation and employer’s liability insurance for the jurisdiction where the work is to be performed. In accordance with AAPD 22-01, any work to be performed is subject to the Defense Base Act, the Workers’ Compensation policy must be endorsed to cover such liability. Worker's Compensation Insurance (Defense Base Act) coverage will be obtained in accordance with AIDAR 752.228-3 which has been revised through the approval of Class Deviation No. M-OAA-DEV-AIDAR-22-10c.

2. Comprehensive automobile and vehicle liability insurance covering claims for injuries to members of the public and/or damages to property of others arising from use of motor vehicles, including on-site and off-site operations, and owned, non-owned, or hired vehicles.

3. Commercial General Liability (including products/completed operations and contractual liability coverage) covering claims for injuries to members of the public or damage to property of others arising out of any negligent act or omission by the Subcontractor or of any of its employees, agents, or lower-tier subcontractors.

4. Professional Liability, if Subcontractor is providing professional services, then Subcontractor shall evidence coverage for damages caused by any acts, errors, or omissions arising out of Subcontractor's performance of professional services.

5. Medical Evacuation (Medevac) Services insurance must be provided by Subcontractor must be provided to all U.S. citizen, U.S. resident alien, and Third Country National employees and their authorized dependents (hereinafter—individual) while overseas. The Subcontractor is not required to provide Medevac insurance to eligible employees and their dependents with a health program that includes sufficient MEDEVAC coverage as approved by the USAID Contracting Officer. A waiver from the appropriate USAID Mission or Bureau official is required to forego coverage. The determination must be based on findings that the quality of local medical services.

2.21 Debarment

Offeror certifies that it is not presently debarred, suspended, or proposed for debarment from, and it has not been declared ineligible for or voluntarily excluded itself from participation in, any Federal procurement. Subcontractor will advise EnCompass immediately if any of these conditions arise during the term of the Subcontract.

2.22 Disputes

The provisions of this Subcontract shall be interpreted in accordance with the laws of the State of Maryland without resort to said state's Conflict of Law rule, and in accordance with its fair meaning and not strictly against either party. Pending final resolution of a dispute hereunder, Subcontractor shall proceed diligently with the performance of this Subcontract and in accordance with all the Terms and Conditions contained herein and with the Prime Contractor's direction thereof. Each party shall bear its own costs of processing any dispute hereunder. In no event shall the Subcontractor acquire any direct claim or direct course of action against the United States Government.

2.23 Travel

Local travel. Commuting costs or the relocation of Subcontractor staff from other geographic areas for the purpose of staffing the project are not reimbursable. Travel costs to and from the Subcontractor's staff home to a Government office or offices or to/from one company or subcontractor's building to another will not be reimbursed. Travel for technical personnel on approved STTA and LTTA to missions is reimbursable.

2.24 Taxes

Offeror is responsible for all federal, state or municipal income tax, social security, unemployment or workman's compensation unless required by law. EnCompass shall withhold and remit any amount, regardless of its description as a tax or otherwise, in countries where local laws require that such amounts be withheld and timely remitted. The Subcontractor is responsible for determination of applicable value added tax (VAT) to

services provided under this Agreement, and remittance per the invoicing instructions. VAT amounts invoiced for payment shall comply with the country's VAT regulations.

2.25 Record Retention

Records, documents, program and individual service records and other evidence of compliance with laws and regulations in connection this project shall be maintained by the Subcontractor, as well as accounting and billing procedures subject to this Agreement. Subcontractor shall provide access to these records by authorized employees or agents of the Prime Contractor, or by the United States government, as applicable. Subcontractor shall retain all such records concerning this Agreement for a period of three (3) years after the completion of the applicable Subcontract. The Subcontractor shall also retain the records should any litigation, claim, or audit commence before the expiration of the three-year period, until all litigation, claims or audit findings involving the records have been resolved.

2.26 Data Collection Retention

In accordance with client requirements, the Subcontractor must destroy all data that has been collected as part of this agreement five (5) years after the end date specified on the Subcontract Summary page.

2.27 Deliverables and Technical Reports

Deliverable requirements will be detailed in the agreement and are to be submitted to the Technical Representative or their designee. Subcontractor's failure to submit required deliverables or reports when due, or failure to deliver required work to the reasonable satisfaction of the Technical Representative within the structures as outlined within the agreement may result in the withholding of payment under the agreement until resolved, or unless such failure arises out of causes beyond the control and without the fault or negligence of the Subcontractor.

2.28 Conflicts of Interest

Offeror warrants to its best knowledge and belief that there are no relevant facts or circumstances which could give rise to a conflict of interest or that such relevant information has been disclosed by the Subcontractor. If an actual or potential conflict of interest is discovered after the execution of this Agreement, Subcontractor will make a full disclosure in writing to the Contracts Manager. The Subcontractor will provide a description of activities it has taken or proposes to take, to avoid, mitigate, or neutralize the actual or potential conflict.

2.29 Right to Publish/Release of Information

Offeror agrees that it will not publish or disseminate any information resulting from the work being performed under this Agreement without providing the Prime Contractor a reasonable period of time to review prior to publishing. Both parties mutually agree not to use the other party's name or reference the other party or its

employees in news releases, publications, advertising, speeches, technical papers, photographs, sales promotions, or publicity purposes from the work performed under this agreement, without prior written approval of the other party. The use of either party's name may be made in internal documents, annual reports, and data bases that are made publicly available as a result of the work performed under this contract. Both parties also agree not to use any proprietary information belonging to the other party, except as authorized by the requesting party. EnCompass' client may use data or information provided by the Subcontractor, subject to any copyright of such materials and identifying notices, provided the identification permissible and no provisions set forth in this agreement or the flow down clauses restrict or prohibit copyright or notice or legend.

2.30 Excusable Delays

Neither Party shall be in default because of any failure to perform under the terms of this Agreement if the failure arises from any incident or circumstance beyond the affected Party's control. Under Federally funded awards, a United States (U.S.) government shutdown and any interruption in the U.S. government's operations shall constitute an incident or circumstance beyond the affected Party's control. Under this circumstance, the affected Party shall inform the other Party immediately, specifying the duration and contingencies. The affected Party shall resolve such contingencies to ensure the performance of its obligations under this Agreement can be resumed as soon as possible.

2.31 Cloud Computing

(a) Definitions. As used in this special contract requirement-
"Cloud computing" means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This includes other commercial terms, such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. It also includes commercial offerings for software-as-a-service, infrastructure-as-a-service, and platform-as-a-service.

"Federal information" means information created, collected, processed, disseminated, or disposed of by or for the Federal Government, in any medium or form. (OMB A-130)

"Information" means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

"Information Security Incident" means an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2)

constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

“Privacy Incident means a violation or imminent threat of violation of security policies, acceptable use policies, or standard security practices, involving the breach of Personally Identifiable Information (PII), whether in electronic or paper format.

“Spillage” means a security incident that results in the transfer of classified or other sensitive or sensitive but unclassified information to an information system that is not accredited (i.e., authorized) for the applicable security level of the data or information. “Cloud Service Provider” or CSP means a company or organization that offers some component of cloud computing – typically Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS) – to other businesses, organizations or individuals.

“Penetration Testing” means security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network. (NIST SP 800-115)

“Third Party Assessment Organizations” means an organization independent of the organization whose IT system is being assessed. They are required to meet the ISO/IEC 17020:1998 standards for independence and managerial competence and meet program requirements for technical FISMA competence through demonstrated expertise in assessing cloud-based solutions.

“Personally Identifiable Information (PII)” means information that can be used to distinguish or trace an individual's identity, such as their name, Social Security Number (SSN), biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual. PII examples include name, address, SSN, or other identifying number or code, telephone number, and e-mail address. PII can also consist of a combination of indirect data elements such as gender, race, birth date, geographic indicator (e.g., zip code), and other descriptors used to identify specific individuals. When defining PII for USAID purposes, the term “individual” refers to a citizen of the United States or an alien lawfully admitted for permanent residence.

(b) Applicability

This special contract requirement applies to the Contractor and all personnel providing support under this contract (hereafter referred to collectively as “Contractor”) and addresses specific USAID requirements in addition to those included in the Federal Acquisition Regulation (FAR), Privacy Act of 1974 (5 U.S.C. 552a - the Act), EGovernment Act of 2002 - Section 208 and Title III, Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Pub. L. 104-191, 110 Stat.

1936), the Sarbanes-Oxley Act of 2002 (SOX, Pub. L. 107-204, 116 Stat 745), National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) and the 800-Series Special Publications (SP), Office of Management and Budget (OMB) memorandums, and other laws, mandates, or executive orders pertaining to the development and operations of information systems and the protection of sensitive information and data.

(c) Limitations on access to, use and disclosure of, Federal information.

(1) The Contractor shall not access, use, or disclose Government data unless specifically authorized by the terms of this contract issued hereunder.

(i) If authorized by the terms of this contract issued hereunder, any access to, or use or disclosure of, Federal information shall only be for purposes specified in this contract.

(ii) The Contractor shall ensure that its employees are subject to all such access, use, and disclosure prohibitions and obligations.

(iii) These access, use, and disclosure prohibitions and obligations shall remain effective beyond the expiration or termination of this contract.

(2) The Contractor shall use related Federal information only to manage the operational environment that supports the Federal information and for no other purpose unless otherwise permitted with the prior written approval of the Contracting Officer.

(d) Records Management and Access to Information

(1) The Contractor shall support a system in accordance with the requirement for Federal agencies to manage their electronic records in accordance with capabilities such as those identified in the provisions of this contract and National Archives and Records Administration (NARA) retention policies.

(2) Upon request by the government, the Contractor shall deliver to the Contracting Officer all Federal information, including data schemas, metadata, and other associated data artifacts, in the format specified in the schedule or by the Contracting Officer in support of government compliance requirements to include but not limited to Freedom of Information Act, Privacy Act, e-Discovery, e- Records and legal or security investigations.

(3) The Contractor shall retain and maintain all Federal information in accordance with records retention provisions negotiated by the terms of the contract and in accordance with USAID records retention policies.

(4) The Contractor shall dispose of Federal information in accordance with the terms of the contract and provide the confirmation of disposition to the Contracting Officer in accordance with contract closeout procedures.

(e) Notification of third party access to Federal information: The Contractor shall notify the Government immediately of any requests from a third party for access to Federal information or, including any warrants, seizures, or subpoenas it receives, including those from another Federal, State, or Local agency, that could result in the disclosure of any Federal information to a third party. The Contractor shall cooperate with the Government to take all measures to protect Federal information from any loss or unauthorized disclosure that might reasonably result from the execution of any such request, warrant, seizure, subpoena, or similar legal process.

(f) Spillage and Information Security Incidents: Upon written notification by the Government of a spillage or information security incident involving classified information, or the Contractor's discovery of a spillage or security incident involving classified information, the Contractor shall immediately (within 30 minutes) notify CIO-HELPDESK@usaid.gov and the Office of Security at SECinformationsecurity@usaid.gov to correct the spillage or information security incident in compliance with agency-specific instructions. The Contractor will also notify the Contracting Officer or Contracting Officer's Representative and the Contractor Facilities Security Officer. The Contractor will abide by USAID instructions on correcting such a spill or information security incident. For all spills and information security incidents involving unclassified and/or SBU information, the protocols outlined above in section (g) and (h) below shall apply.

(g) Information Security Incidents

(1) Security Incident Reporting Requirements: All Information Security Incidents involving USAID data or systems must be reported in accordance with the requirements below, even if it is believed that the information security incident may be limited, small, or insignificant. USAID will determine the magnitude and resulting actions.

(i) Contractor employees must report via e-mail all Information Security Incidents to the USAID Service Desk immediately, but not later than 30 minutes, after becoming aware of the Incident, at: CIOHELPDESK@usaid.gov, regardless of day or time, as well as the Contracting Officer and Contracting Officer's representative and the Contractor Facilities Security Officer.

Contractor employees are strictly prohibited from including any Sensitive Information in the subject or body of any e-mail concerning information security incident reports. To transmit Sensitive Information, Contractor employees must use FIPS 140-2 compliant encryption methods to protect Sensitive Information in attachments to email. Passwords must not be communicated in the same email as the attachment.

(ii) The Contractor must provide any supplementary information or reports related to a previously reported information security incident directly to CIO-HELPDESK@usaid.gov, upon request. Correspondence must

include related ticket number(s) as provided by the USAID Service Desk with the subject line "Action Required: Potential Security Incident".

(h) Privacy Incidents Reporting Requirements: Privacy Incidents may result in the unauthorized use, disclosure, or loss of personally identifiable information, and can result in the loss of the public's trust and confidence in the Agency's ability to safeguard personally identifiable information. PII breaches may impact individuals whose PII is compromised, including potential identity theft resulting in financial loss and/or personal hardship experienced by the individual. Contractor employees must report by e-mail all Privacy Incidents to the USAID Service Desk immediately (within 30 minutes), after becoming aware of the Incident, at: CIO-HELPDESK@usaid.gov, regardless of day or time, as well as the USAID Contracting Officer or Contracting Officer's representative and the Contractor Facilities Security Officer. If known, the report must include information on the format of the PII (oral, paper, or electronic.) The subject line shall read "Action Required: Potential Privacy Incident".

(i) Information Ownership and Rights: USAID information stored in a cloud environment remains the property of USAID, not the Contractor or cloud service provider (CSP). USAID retains ownership of the information and any media type that stores Federal information. The CSP shall only use the Federal information for purposes explicitly stated in the contract. Further, the cloud service provider shall export Federal information in a machine readable and non-proprietary format that USAID requests at the time of production, unless the parties agree otherwise.

(j) Security Requirements:

(1) The Contractor shall adopt and maintain administrative, technical, operational, and physical safeguards and controls that meet or exceed requirements contained within the Federal Risk and Authorization Management Program (FedRAMP) Cloud Computing Security Requirements Baseline, current standard for NIST 800-53 (Security and Privacy Controls for Federal Information Systems) and Organizations, including Appendix J, and FedRAMP Continuous Monitoring Requirements for the security level and services being provided, in accordance with the security categorization or impact level as defined by the government based on the Federal Information Processing Standard (FIPS) Publication 199 (FIPS-199).

(2) The Contractor shall comply with FedRAMP requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the security assessment and authorization (SA&A) is based on the system's complexity and security categorization. The Contractor shall create, maintain and update the following documentation using FedRAMP requirements and templates, which are available at https://www.FedRAMP.gov.

(3) The Contractor must support SA&A activities to include assessment by an accredited Third Party Assessment Organization (3PAO) initially and whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan. The Contractor must make available to

the Contracting Officer, the most current, and any other, Security Assessment Reports for consideration as part of the Contractor's overall Systems Security Plan.

(4) The Government reserves the right to perform penetration testing or request Penetration Testing by an independent source. If the Government exercises this right, the Contractor shall allow Government employees (or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with FedRAMP requirements. Review activities include but are not limited to scanning operating systems, web applications, databases, wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Federal information for vulnerabilities.

(5) Identified gaps between required FedRAMP Security Control Baselines and Continuous Monitoring controls and the Contractor's implementation as documented in the Security Assessment Report must be tracked by the Contractor for mitigation in a Plan of Action and Milestones (POA&M) document.

Depending on the severity of the gaps, the Government may require them to be remediated before any restricted authorization is issued.

(6) The Contractor is responsible for mitigating all security risks found during SA&A and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within thirty (30) calendar days and all moderate risk vulnerabilities must be mitigated within sixty (60) calendar days from the date vulnerabilities are formally identified. USAID may revoke an ATO for any system if it is determined that the system does not comply with USAID standards or presents an unacceptable risk to the Agency. The Government will determine the risk rating of vulnerabilities.

(7) The Contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance with the requirements and to allow for appropriate risk decisions for an Information Technology security program. The Government reserves the right to conduct onsite inspections. The Contractor must make appropriate personnel available for interviews and provide all necessary documentation during this review and as necessary for continuous monitoring activities.

(k) Privacy Requirements: Cloud Service Provider (CSP) must understand and adhere to applicable federal Privacy laws, standards, and guidance to protect Personally Identifiable Information (PII) about individuals that will be collected and maintained by the Contractor solution. The Contractor responsibilities include full cooperation for any request for disclosure, subpoena, or other judicial process seeking access to records subject to the Privacy Act of 1974.

(l) Data Location: The Contractor must disclose the data server locations where the Agency data will be stored as well as the redundant server locations. The Contractor must have prior Agency approval to store Agency data in locations outside of the United States.

(m) Terms of Service (ToS): The Contractor must disclose any requirements for terms of service agreements and clearly define such terms prior to contract award. All ToS provisions regarding controlling law, jurisdiction, and indemnification must align with Federal statutes, policies, and regulations.

(n) Service Level Agreements (SLAs): The Contractor must be willing to negotiate service levels with USAID; clearly define how performance is guaranteed (such as response time resolution/mitigation time, availability, etc.); monitor their service levels; provide timely notification of a failure to meet the SLAs; and evidence that problems have been resolved or mitigated. Additionally, at USAID's request, the Contractor must submit reports or provide a dashboard where USAID can continuously verify that service levels are being met. Where SLAs fail to be met, USAID may assess monetary penalties or service credit.

(o) Trusted Internet Connection (TIC): The Contractor must route all USAID traffic through the TIC.

(p) Forensics, Freedom of Information Act (FOIA), Electronic Discovery, or additional Information Requests: The Contractor must allow USAID access required to retrieve information necessary for FOIA and Electronic Discovery activities, as well as, forensic investigations for both criminal and noncriminal purposes without their interference in these activities. USAID may negotiate roles and responsibilities for conducting these activities in agreements outside of this contract.

(1) The Contractor must ensure appropriate forensic tools can reach all devices based on an approved timetable.

(2) The Contractor must not install forensic software or tools without the permission of USAID.

(3) The Contractor, in coordination with USAID Bureau for Management, Office of The Chief Information Officer (M/CIO)/ Information Assurance Division (IA), must document and preserve data required for these activities in accordance with the terms and conditions of the contract.

(4) The Contractor, in coordination with USAID M/CIO/IA, must clearly define capabilities, procedures, roles and responsibilities and tools and methodologies for these activities.

(q) The Contractor shall include the substance of this special contract requirement, including this paragraph (p), in all subcontracts, including subcontracts for commercial items.

2.32AIDAR 752.204-72 Access to USAID Facilities and USAID's Information Systems

(a) HSPD-12 and Personal Identity Verification (PIV). Individuals engaged in the performance of this award as employees, consultants, or volunteers of the contractor must comply with all applicable Homeland Security

Presidential Directive-12 (HSPD-12) and Personal Identity Verification (PIV) procedures, as described below, and any subsequent USAID or Government-wide HSPD-12 and PIV procedures/policies.

(b) A U.S. citizen or resident alien engaged in the performance of this award as an employee, consultant, or volunteer of a U.S firm may obtain access to USAID facilities or logical access to USAID's information systems only when and to the extent necessary to carry out this award and in accordance with this clause. The contractor's employees, consultants, or volunteers who are not U.S. citizens or resident aliens as well as employees, consultants, or volunteers of non-U.S. firms, irrespective of their citizenship, will not be granted logical access to U.S. Government information technology systems (such as Phoenix, GLAAS, etc.) and must be escorted to use U.S. Government facilities (such as office space).

(c) (1) No later than five business days after award, the Contractor must provide to the Contracting Officer's Representative (COR) a complete list of employees that require access to USAID facilities or information systems. (2) Before a contractor (or a contractor employee, consultant, or volunteer) or subcontractor at any tier may obtain a USAID ID (new or replacement) authorizing the individual routine access to USAID facilities in the United States, or logical access to USAID's information systems, the individual must provide two forms of identity source documents in original form to the Enrollment Office personnel when undergoing processing. One identity source document must be a valid Federal or State Government-issued picture ID. Contractors may contact the USAID Security Office to obtain the list of AAPD 16-02 Special Requirements for Information Technology (IT) 2 acceptable forms of documentation. Submission of these documents, to include documentation of security background investigations, is mandatory in order for the contractor to receive a PIV/Facilities Access Card (FAC) card and be granted access to any of USAID's information systems. All such individuals must physically present these two source documents for identity proofing at their enrollment.

(d) The Contractor must send a staffing report to the COR by the fifth day of each month. The report must contain the listing of all staff members with access that separated or were hired under this contract in the past sixty (60) calendar days. This report must be submitted even if no separations or hiring occurred during the reporting period. Failure to submit the 'Contractor Staffing Change Report' each month may, at USAID's discretion, result in the suspension of all logical access to USAID information systems and/or facilities access associated with this contract. USAID will establish the format for this report.

(e) Contractor employees are strictly prohibited from sharing logical access to USAID information systems and Sensitive Information. USAID will disable accounts and revoke logical access to USAID IT systems if Contractor employees share accounts.

(f) USAID, at its discretion, may suspend or terminate the access to any systems and/or facilities when a potential Information Security Incident or other electronic access violation, use, or misuse incident gives cause for such action. The suspension or termination may last until such time as USAID determines that the situation has been corrected or no longer exists.

(g) The Contractor must notify the COR and the USAID Service Desk at least five business days prior to the Contractor employee's removal from the contract. For unplanned terminations of Contractor employees, the Contractor must immediately notify the COR and the USAID Service Desk (CIOHELPDESK@usaid.gov or (202) 712-1234). The Contractor or its Facilities Security Officer must return USAID PIV/FAC cards and remote authentication tokens issued to Contractor employees to the COR prior to departure of the employee or upon completion or termination of the contract, whichever occurs first.

(h) The contractor is required to insert this clause including this paragraph (h) in any subcontracts that require the subcontractor, subcontractor employee, or consultant to have routine physical access to USAID space or logical access to USAID's information systems.

2.33 Limitation on Acquisition of Information Technology

a) Definitions. As used in this contract -- "Information Technology" means
(1) Any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency; where
(2) such services or equipment are ' used by an agency' if used by the agency directly or if used by a contractor under a contract with the agency that requires either use of the services or equipment or requires use of the services or equipment to a significant extent in the performance of a service or the furnishing of a product.
(3) The term " information technology" includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including provisioned services such as cloud computing and support services that support any point of the lifecycle of the equipment or service), and related resources.
(4) The term "information technology" does not include any equipment that is acquired by a contractor incidental to a contract that does not require use of the equipment.
(b) The Federal Information Technology Acquisition Reform Act (FITARA) requires Agency Chief Information Officer (CIO) review and approval of contracts that include information technology or information technology services.
(c) The Contractor must not acquire information technology as defined in this clause without the prior written approval by the contracting officer as specified in this clause.
(d) Request for Approval Requirements: Clauses And Special Contract Requirements For Facilities Access, Security, and Information Technology (IT) (Class Deviations M/OAA-DEV-FAR-18-2c, and M/OAA-DEVAIDAR-18-2c) 8 (1) If the Contractor determines that any information technology will be necessary to meet the Government's requirements or to facilitate activities in the Government's statement of work, the Contractor must request prior written approval from the Contracting Officer. (2) As part of the request, the Contractor must provide the Contracting Officer a description and an estimate of the total cost of the information technology equipment, software, or services to be procured under this contract. The Contractor must

simultaneously notify the Contracting Officer's Representative (COR) and the Office of the Chief Information Office at ITAuthorization@usaid.gov.

(e) The Contracting Officer will provide written approval to the Contractor through modification to the contract expressly specifying the information technology equipment, software, or services approved for purchase by the COR and the Agency CIO. The Contracting Officer will include the applicable clauses and special contract requirements in the modification.

(f) Except as specified in the contracting officer's written approval, the Government is not obligated to reimburse the Contractor for any costs incurred for information technology as defined in this clause.

(g) The Contractor must insert the substance of this clause, including this paragraph (g), in all subcontracts.

3 INSTRUCTIONS TO OFFERORS

EnCompass requests proposals by the issue of this RFP for the supply of services as specified in Part I.

3.1 Due Date

Your proposal is due electronically with all required signatures, no later than the date noted in the RFP Schedule above. Please be advised that late or incomplete submissions may be considered non-responsive and may not be considered for award.

3.2 Proposal Validity Period

The Offeror's proposals will be considered valid for 60 days after submission.

3.3 Responsibility for Compliance with Legal Requirements

The offeror's products, services, and facilities shall be in full compliance with all applicable federal, and local laws, regulation, codes, standards, and ordinances, regardless of whether or not they are referred to by herein. The submission of a proposal to EnCompass in response to this RFP constitutes an offer to which the Offeror agrees to the terms and conditions in this RFP and any attachments.

3.4 Reservation of Rights

EnCompass reserves the right to not issue an award based on proposals received in response to this RFP. EnCompass reserves the right to cancel this procurement at any time without prior notice, and to reject any or all responses received.

The RFP does not commit EnCompass to make any award or to pay any costs incurred in the preparation and submission of the proposal. EnCompass may cancel this RFP or any part of it. EnCompass reserves the right to reject any and all proposals, and to waive any informality in received proposals. In addition, EnCompass reserves the right to establish a competitive range of one or more Offerors and conduct further negotiations concerning price and other terms before awarding the contract, or to award without discussions.

An Offeror selected under this solicitation is not authorized to incur costs prior to receiving EnCompass' written authorization.

EnCompass requires that Offerors observe the highest standard of ethics during the procurement and execution of subcontracts. In pursuance of this policy, EnCompass defines the terms set forth below as follows:

- "Corrupt practice" means the offering, giving, receiving or soliciting, directly or indirectly, of anything of value to influence the action of an EnCompass individual in the procurement process or contract execution

- "Fraudulent practice" means a misrepresentation or omission of facts in order to influence a procurement process or the execution of a contract
- “Collusive practices” means a scheme or arrangement between two or more Offerors, with or without the knowledge of EnCompass, designed to establish prices at artificial, noncompetitive levels
- “Coercive practices” means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation in a procurement process, or affect the execution of a contract

EnCompass will reject a recommendation for award if it determines that the Offeror recommended for award has, directly or through an agent, engaged in corrupt, fraudulent, collusive, or coercive practices in competing for the contract in question.

3.5 Eligibility and Size Designation

Offerors shall provide evidence to verify that they:

- Have the legal capacity to enter into a subcontract with EnCompass
- Are not insolvent or bankrupt, and have not had their business activities suspended or been the subject of legal proceedings for any of the foregoing
- Have fulfilled and are up to date with their tax and legal obligations
- Are registered in SAM.gov, a CAGE/NCAGE and a Unique ID (UEI) number

The Offeror must have at least 5 years of experience providing corporate security services as described in section 1.3 Scope of Work.

3.6 RFP Clarifications and Amendments

An Offeror may request clarification of the RFP terms in English by e-mail to mrichardson@encompassworld.com no later than Friday August 23, 2024 at 5 p.m. EST. EnCompass will respond in writing by email to all requests for clarification, provided that such requests are received by the date and time indicated. Should a clarification result in changes to the RFP, EnCompass will issue an amendment if necessary.

At any time prior to the deadline for submission of proposals, EnCompass may modify the RFP by issuing an amendment. Any amendment issued shall be part of the RFP and will be communicated in writing by email to all Offerors. To give prospective Offerors a reasonable period to incorporate the amendment terms in their proposals, EnCompass may, at its discretion, extend the deadline for the submission of proposals in writing.

3.7 Cost of Preparation of Proposals

Offerors are responsible for all costs incurred in preparing or responding to this RFP. All materials and

documents submitted in response to this RFP become the property of EnCompass. This RFP does not obligate EnCompass to compensate for costs associated with the preparation of an Offeror's proposal.

3.8 Language of Proposal

The proposal, as well as all correspondence and documents relating to the proposal the offeror and EnCompass exchange, shall be written in English. Supporting documents that are part of the proposal must be in English.

3.9 Period of Validity of Proposals

Proposals shall remain valid for a period of 60 days after submission. A proposal valid for a shorter period shall be rejected as non-responsive. EnCompass may ask Offerors to extend the validity period of their proposals in writing if necessary.

3.10 Late Proposals

EnCompass will not consider any proposal received after the deadline for submission. Any proposal received after the deadline will be returned to the Offeror with notice of rejection.

3.11 Annulment of RFP

EnCompass reserves the right to annul the proposal process and reject all proposals at any time prior to completion of the procurement process or award, without thereby incurring any liability to Offerors.

3.12 Withdrawal, Substitution, and Modification of Proposals

An Offeror may withdraw, substitute, or modify their proposal after the submission by sending a written notice, duly signed by an authorized representative. Proposals requested to be withdrawn will be returned unopened to the Offerors.

No proposal may be withdrawn, substituted, or modified in the interval between the deadline for submission of proposals and expiry of the period of proposal validity.

3.13 Confidentiality

Information related to the examination, evaluation, comparison, and post-qualification of proposals, and recommendation of award shall not be disclosed to Offerors, or any other persons not officially concerned with this RFP process, until information on award is communicated to all Offerors.

Any effort by an Offeror to influence EnCompass in the examination, evaluation, comparison, and post-qualification of an offer or an award decision will result in the rejection of their proposal.

From the proposal opening to award, Offerors may contact EnCompass on any matter related to the RFP process in writing.

3.14 Award Without Discussions

Awards may be made based on initial proposals and without holding discussions.

3.15 Notification of Award

Prior to expiry of the period of proposal validity, the EnCompass shall notify in writing the successful Offerors that their proposals have been accepted. At the same time, Offerors not receiving awards will be notified that they will not receive an award.

3.16 Preparation of Proposals

Offerors will submit the following documentation:

- Volume 1 - Technical Proposal
- Volume 2 – Price/Business Proposal

3.16.1 VOLUME 1 - TECHNICAL PROPOSAL

The Offeror's Technical Proposal must contain the following information and documentation to be considered for award.

1. **Cover Letter**:

A cover letter shall be included with the proposal on the Offeror's company letterhead with a duly authorized signature. The cover letter shall include the following items:

- Contact person
- Name of organization(s) submitting proposal
- Address of organization
- Organization telephone and fax, mobile numbers
- E-mail of contact person
- Acknowledgement of solicitation amendments received
- Certification of a 60-day validity period for proposed prices

2. **Executive Summary** (not to exceed 1 page)

Offers must summarize the Offeror's overarching approach they will take to providing the services requested herein. Offeror must briefly describe their organization's ability to undertake activities, as well as technical and managerial resources of the organization.

3. **Technical Approach to Scope of Work** (not to exceed 3 pages, inclusive of graphs and tables).

Offerors must provide a detailed description of their capabilities and expertise that relate to the Statement of Work listed in Section 1.3. Offeror must describe their technical approach to each of the services below. If the Offeror specializes in some but not all of these service areas, specify this in the Technical Capabilities section. Offerors will not be excluded from consideration because they do not have capacity in every sector and/or service area noted in this RFP, including experience in:

- Security assessments of office spaces and residences
- Security monitoring and clear/concise English communication of threats to teams
- Journey management plan development
- Safety and Security Plan development
- Provision of security trainings, including crisis management and first aid expertise Physical presence in Ukraine, in line with the requirement in the Scope of Work
- Prior experience providing security services and support to USAID funded activities in Ukraine

4. **Management plan** (not to exceed 2 pages, inclusive of graphs and tables)

The Offeror shall propose a management plan and staffing pattern that includes necessary technical, administrative, and support staff, accompanied by one Curriculum vitae (CV) per position/labor category for personnel who represent the top capabilities of the Offeror in that role. CVs should include details regarding education and relevant experience, skills, and credentials.

The offeror shall:

- Describe the organization's management structure that will support the subcontracted activities.
- Describe the organization's ability to perform the requested services in Ukraine.
    - Provide a staffing chart that lists all proposed and required positions and their roles/tasks.
    - In an Attachment to Volume 1, include one CV per position (not to exceed 2 pages each) demonstrating the top capabilities of the Offeror for each of the positions in Exhibit 1. No more than 6 CVs should be submitted. CVs should include the following:
        - Education/degrees
        - Positions and experience, along the lines of service areas noted in the RFP

Exhibit 1: Position Descriptions (requirements)

Position	Role/Experience
Security Program Manager	***Role**:* • Provide oversight and contract management ***Experience**:* • A minimum of 10 years of security services and project management experience • Demonstrated experience in conflict environments
Country Security Manager	***Role**:*

Position	Role/Experience
	● Provide in country support to the UMLS office and staff ● Prepare JMPs, conduct site visits and assessments, provide briefings and trainings on demand ● Oversee routine security activities such as signal check ins ● Coordinate with EnCompass CMT and UMLS COP and Operations teams ***Experience**:* ● A minimum of 8 years of experience relevant to SOW activities ● Extensive expertise in conflict environments, familiarity with the current Ukrainian security context.
Security Coordinator	***Role***: ● Support Country Security manager in tasks including, but not limited to: ○ Providing in country support to the UMLS office and staff ○ Preparation of JMPs, site visits and assessments, briefings and trainings ○ Conducting routine security activities ***Experience**:* ● A minimum of 5 years of experience relevant to SOW activities ● Experience in conflict environments, familiarity with the current Ukrainian security context.
Analyst	***Role**:* ● Support security research and monitoring tasks including weekly and quarterly reporting, site assessments, etc. ***Experience**:* ● A minimum of 3 years of experience relevant to SOW activities
OTHER ROLES	Up to two additional positions may be proposed by the offeror based on the scope of work. The role and experience requirements for proposed positions should be clearly described in the Management Plan. The contractor may also detail or provide additional specification to the suggested roles to reflect their organizational structure.

5. Past Performance

Provide a concise summary of the organization's past and present projects that have a direct relevance to the service areas noted in the RFP:

- Minimum of 3 and not more than 5 projects with detailed description of project value, period of performance, principal activities and results, client, and client contact information for references.
- Provide a description of any publications or reports that demonstrate organization's special qualifications and experience that relate directly to Scope of Work. The Past Performance format is attached (Attachment A).

3.16.2 VOLUME 2 – PRICE/BUSINESS PROPOSAL

1. Legal Documents

Offerors must submit the following documentation to meet the requirements of the RFP.

- Incorporation or business registration
- Registration in SAM.gov or proof of the ability to register in SAM.gov
- The registration documentation must prove at least 3 years of existence
- Certified financial statements of the last three years to demonstrate financial soundness
- Completed and signed Representations and Certifications (Attachment B)
- Completed EnCompass Subcontractor/Vendor Questionnaire, Parts 1 and 2 (Attachment C)

Photocopies of these documents must be legible and complete.

2. Proposed Prices

Offerors are to propose burdened billing rates for all labor services needed to carry out any activity as described in the Scope of Work. Prices must be submitted in USD. . All positions below are part-time and can bill no more than the LOE negotiated. EnCompass will accept prorated or proportional share of other costs related to employment.

The Offeror will provide the following elements:

- Burdened Billing Rates for staff and services; the burdened billing rates must be presented as daily rates

  Definition of Burdened Rates: Rates that include base salary plus any and all indirect costs, such as fringe, overhead, fees, and any other benefits.

  The burdened daily rates will be fixed for the life of the subcontract. Offerors can propose an escalation to their rates for the second year of the award.

- Travel and Other Direct Costs

  Offerors shall use the annual budget format provided below to supply details on their proposed Labor Category rates and proposed ODCs.

Year 1: October 24, 2024 – October 23, 2025

Labor			
Labor Category	**Year 1 Burdened Daily Rate**	**Proposed LOE**	**Total Cost $**
Security Program Manager			
Country Security Manager			

Security Coordinator			
Analyst			
		Total Year 1 Labor Cost	

Other Direct Costs	
ODC line item	Total Cost $
Travel and General	
[propose additional line items as needed]	
Total Year 1 ODC Cost	$10,000.00

Year 2: October 24, 2025 – October 23, 2026

Labor			
Labor Category	**Year 2 Burdened Daily Rate**	**Proposed LOE**	**Total Cost $**
Security Program Manager			
Country Security Manager			
Security Coordinator			
Analyst			
		Total Year 2 Labor Cost	

Other Direct Costs	
ODC line item	Total Cost $
Travel and General	
[propose additional line items as needed]	
Total Year 2 ODC Cost	$10,000.00

Year 3: October 24, 2026 – March 1, 2027

Labor			
Labor Category	**Year 3 Burdened Daily Rate**	**Proposed LOE**	**Total Cost $**
Security Program Manager			
Country Security Manager			
Security Coordinator			
Analyst			

Total Year 3 Labor Cost	
Other Direct Costs	
ODC line item	Total Cost $
Travel and General	
[propose additional line items as needed]	
Total Year 3 ODC Cost	$5,000.00

The Offeror must provide at least one item of supporting documentation for their proposed Burdened Billing Rates. Documentation that will be accepted are:

- Published price list of staff Burdened Billing Rates
- A redacted contract demonstrating the Burdened Billing Rates the Offeror charges its clients
- A breakdown of each proposed Burdened Billing Rates that shows base salary and all costs included in the burdened rate, or indirect costs that are applied to base salary, such as fringe, overhead, fees, benefits, etc.
- A redacted contract or audited financial statement of established indirect cost rates used to create the Burdened Billing Rates

3.17 Proposal Submission

Offerors must submit two separate files in the specified format by email to the address identified on the cover page of this RFP, and by the date and time stipulated.

Technical Proposals must not make reference to pricing data so that the technical evaluation can be made strictly on the basis of technical merit.

- Volume 1 – Technical Proposal – in Word or in PDF format
- Volume 2 – Price/Business Proposal – in Word or PDF format, and Excel if submitting detailed breakdown of proposed prices

4 PART IV: EVALUATION AND QUALIFICATION CRITERIA

4.1 Criteria

To be acceptable and eligible for evaluation, proposals must be prepared in accordance with Part III– Instructions to Offerors and meet all the requirements set forth in the other sections of this solicitation.

Determination of a proposal's responsiveness will be based on the contents of the proposal itself.

A substantially responsive proposal is one that conforms to all the terms, conditions, and specifications of the RFP without material deviation, reservation, or omission. A material deviation, reservation, or omission is one that:

- Affects in any substantial way the full presentation of services and experiences
- If rectified, would unfairly affect the competitive position of other Offerors presenting substantially responsive proposals

Technical, cost, and other factors will be evaluated relative to each other, as described herein.

The technical proposal will be scored by a technical evaluation committee using the criteria shown later in this section.

The criteria are presented by major category, with relative order of importance, so that Offerors will know which areas require emphasis in the preparation of proposals.

Offerors should note that these criteria serve: (1) as the standard against which all proposals will be evaluated, and (2) to identify the significant matters Offerors should address in their proposals.

The Price/Business proposals will be evaluated for a best-value determination based on the offer's technical score and favorable price comparison and analysis.

The evaluation procedures are set forth below:

1. Initial Evaluation

EnCompass will examine Volumes 1 and 2 to determine the completeness of each, and ensure that the Offeror is qualified and eligible to receive an award. If any of the required legal documents is missing, EnCompass, at its discretion, may contact the Offeror and request they provide the missing legal documentation. Offerors are encouraged to provide justification for any documentation they are not able to provide in the proposal. EnCompass, at its discretion, will take into consideration any justification provided so long as it is sound and EnCompass can meet USAID's procurement requirements.

2. Technical Evaluation (70 points)

After the Initial Evaluation, EnCompass will review the proposals remaining for consideration to determine technical acceptability. EnCompass will consider the following evaluation criteria in determining the acceptability of the technical proposal. To be considered technically acceptable, the technical proposal must conform to the requirements of the solicitation and get at least 55/70 points.

***Technical Approach (25 points) (3 pages)*:**

- A clear understanding of the Scope of Work

- Extent to which the approach is conceptually appropriate, clear, logical, well-conceived, and feasible based on the services the Offeror provides along the lines of the SOW described in this RFP
- Extent to which the approach demonstrates a clear, concise, and approach to capacity development and training.
- Offerors are encouraged to explain their methodology for accomplishing service areas set forth in the SOW. How an offeror sets out to create internal and external reports, JMPs or security plans for example.

Management Plan and Staffing (20 points) (1.5 pages):

- Extent to which management structure ensures effective management of subcontract activities leading to quality and timely delivery, accounting for complex and often fluctuating environment
- Extent to which management structure demonstrates ability to mobilize and provide the described services
- Demonstrates the staff have the required qualifications and experience as listed in the position descriptions in **Exhibit 1**

Experience and Past Performance (25 points):

Offeror must prove relevant past performance information for the previous 3 years for at least 3 similar projects (and not more than 5) indicating relevant work performed:

- Experience in Ukraine is required
- Experience in additional conflict/war zones required
- Experience drafting documentation as outlined in the SOW required
- Experience providing advisory services as outlined in the SOW required, including these services listed on Pages 3 and 4.
- Experience with USAID contractors is preferred, including support to in-country staffing, including USN/TCNs.

EnCompass will check references. The Offeror must include this information in the template provided as Attachment A.

3. Price/Business Proposal Evaluation

The price evaluation will include:

- Analysis of the reasonability of prices proposed
- Comparison of Offeror's prices proposed and prices for same/similar services needed

Prices deemed advantageous to EnCompass will support a best-value award of highly rated technical proposals and services that are cost-shared between UMLS and other entities.

4.2 Determination of Competitive Range and Award

1. Competitive Range

Competitive Range may be established for the most highly rated proposals with the number of proposals in the competitive range to be determined.

EnCompass may limit offers in the competitive range to the greatest number that will permit efficient competition among the most highly rated offers. EnCompass may exclude an offer if it is so deficient as to essentially require a new technical proposal. EnCompass may exclude an offer with unreasonable prices in relation to more competitive offers. EnCompass may exclude an offer requiring extensive discussions, a complete rewrite, or major revisions, such as to allow an Offeror unfair advantage over more competitive offers.

EnCompass intends to issue one award resulting from this solicitation to the responsible Offerors whose proposals represent the best value after evaluation in accordance with the factors in this solicitation.

2. Award Criteria

Proposals that represent the best value will be eligible for award. Best value will be offers that provide the greatest overall benefit in response to the requirements: high technical score, and acceptable and reasonable prices after analysis and comparison.

A technical and price trade-off analysis will be performed to determinate the best value to the program. EnCompass will not select an offer for award on the basis of a superior technical proposal without consideration of the prices proposed.

If deemed necessary, the EnCompass will visit the offices of the selected firms to confirm organizational and accounting capacity as recorded on the EnCompass Subcontractor/Vendor Questionnaire, Attachment C. The EnCompass team will validate the responses the firm provided on the Questionnaire, and record any changes to the responses.

The EnCompass team, in consultation with the home office Contracts Representative (and others as designated), will compare proposed prices and make a determination that the rates are reasonable, or request a best and final offer on the proposed prices.

3. Responsibility Determination

Prior to entering into any type of agreement with an Offeror, EnCompass will ensure the Offeror's responsibility, by reviewing the following:

1. Evidence of a UEI number, CAGE/NCAGE code, and SAM.gov registration
2. The source, origin and nationality of the products or services are not from a Prohibited Country (explained below).
3. Offeror has adequate financial resources to finance and perform the work or deliver goods or the ability to obtain financial resources.
4. Ability to comply with required or proposed delivery or performance schedules.
5. A satisfactory past performance record.
6. A satisfactory record of integrity and business ethics.
7. Offeror has the necessary organization, experience, accounting and operational controls and technical skills.
8. Is qualified and eligible to perform work under applicable laws and regulations.

5 LIST OF ATTACHMENTS

ATTACHMENT A: PAST PERFORMANCE FORM

ATTACHMENT B: REPRESENTATIONS AND CERTIFICATIONS

ATTACHMENT C: ENCOMPASS VENDOR/SUBCONTRACTOR QUESTIONNAIRE

LINKS TO REQUIRED POLICY

ATTACHMENT A

Past Performance Form	
Name of Contracting Client	
Contract Type	
Contract No.	
Period of Performance	
Contract value – award amount	
Client Contact Name:	
Client Contact Telephone No.	
Client Contact E-Mail Address	
Description of Work/Services	
Results (Describe specific results achieved)	
Issues *(If problems were encountered on this contract, provide explanation on corrective action taken)*	

ATTACHMENT B – REPRESENTATIONS AND CERTIFICATIONS

52.204-24 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (Nov 2021)

The Offeror shall not complete the representation at paragraph (d)(1) of this provision if the Offeror has represented that it "does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument" in paragraph (c)(1) in the provision at 52.204-26, Covered Telecommunications Equipment or Services—Representation, or in paragraph (v)(2)(i) of the provision at 52.212-3, Offeror Representations and Certifications-Commercial Products or Commercial Services. The Offeror shall not complete the representation in paragraph (d)(2) of this provision if the Offeror has represented that it "does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services" in paragraph (c)(2) of the provision at 52.204-26, or in paragraph (v)(2)(ii) of the provision at 52.212-3.

(a) Definitions. As used in this provision—

Backhaul, covered telecommunications equipment or services, critical technology, interconnection arrangements, reasonable inquiry, roaming, and substantial or essential component have the meanings provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) Prohibition. (1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. Nothing in the prohibition shall be construed to—
(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Cover telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract or extending or renewing a contract with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract. Nothing in the prohibition shall be construed to—

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Cover telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(c) Procedures. The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (https://www.sam.gov) for entities excluded from receiving federal awards for "covered telecommunications equipment or services".

(d) Representation. The Offeror represents that—

(1) It □ will, □ will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation. The Offeror shall provide the additional disclosure information required at paragraph (e)(1) of this section if the Offeror responds "will" in paragraph (d)(1) of this section; and

(2) After conducting a reasonable inquiry, for purposes of this representation, the Offeror represents that—

It □ does, □ does not use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services. The Offeror shall provide the additional disclosure information required at paragraph (e)(2) of this section if the Offeror responds "does" in paragraph (d)(2) of this section.

(e) Disclosures. (1) Disclosure for the representation in paragraph (d)(1) of this provision. If the Offeror has responded "will" in the representation in paragraph (d)(1) of this provision, the Offeror shall provide the following information as part of the offer:
(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the original equipment manufacturer (OEM) or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(ii) For covered services—

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the Product Service Code (PSC) of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(2) Disclosure for the representation in paragraph (d)(2) of this provision. If the Offeror has responded "does" in the representation in paragraph (d)(2) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(ii) For covered services—

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the PSC of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(End of provision)

52.204-26 Covered Telecommunications Equipment or Services-Representation (Oct 2020)

(a) Definitions. As used in this provision, "covered telecommunications equipment or services" and "reasonable inquiry" have the meaning provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) Procedures. The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (https://www.sam.gov) for entities excluded from receiving federal awards for "covered telecommunications equipment or services".

(c) (1) Representation. The Offeror represents that it □ does, □ does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument.

(2) After conducting a reasonable inquiry for purposes of this representation, the offeror represents that it □ does, □ does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services.

(End of provision)

52.204-27 Prohibition on a ByteDance Covered Application (June 2023)

Vendor certifies to the following restrictions:

(a) Definitions. As used in this clause—

Covered application means the social networking service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited.

Information technology, as defined in 40 U.S.C. 11101(6)—

(1) Means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use—

(i) Of that equipment; or

(ii) Of that equipment to a significant extent in the performance of a service or the furnishing of a product;

(2) Includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but

(3) Does not include any equipment acquired by a Federal contractor incidental to a Federal contract.

(b) Prohibition. Section 102 of Division R of the Consolidated Appropriations Act, 2023 (Pub. L. 117-328), the No TikTok on Government Devices Act, and its implementing guidance under Office of Management and Budget (OMB) Memorandum M-23-13, dated February 27, 2023, "No TikTok on Government Devices" Implementation Guidance, collectively prohibit the presence or use of a covered application on executive agency information technology, including certain equipment used by Federal contractors. The Contractor is prohibited from having or using a covered application on any information technology owned or managed by the Government, or on any information technology used or provided by the Contractor under this contract, including equipment provided by the Contractor's employees; however, this prohibition does not apply if the Contracting Officer provides written notification to the Contractor that an exception has been granted in accordance with OMB Memorandum M-23-13.

(c) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (c), in all subcontracts, including subcontracts for the acquisition of commercial products or commercial services.

(End of clause)

ATTACHMENT C: SUBCONTRACTOR/VENDOR QUESTIONNAIRE

ENCOMPASS SUBCONTRACTOR/VENDOR QUESTIONNAIRE		
Check One:	☐ New [a completed W-9 or W-8 must accompany this form] ☐ Address Change	
SUBCONTRACTOR/VENDOR PROFILE AND CAPABILITIES		
Unique Entity ID (SAM) _____	**Legal Name of entity:** Enter legal name **Doing Business As (if applicable):**	**1099 Reportable?** ☒ Yes ☐ No
Do you have:	☐ Employer Identification No. (EIN) ***OR*** _____	☐ Social Security Number _____
Legal Status: (check one)	☐ Corporate (not tax exempt) ☐ Corporate (tax exempt) ☐ Partnership	☐ International Organization (per 26 CFR 1.6049-4) ☐ Individual/Sole Proprietorship or single-member LC ☐ Other:
Type of Business:	☐ Consultant/SME ☐ Service Company ☐ International Consultant/SME	☐ Staffing Company/Contract Labor ☐ Other: _____
Consultants Only:	**Have you had clients over the last 12 months?** ☐ Yes ☐ No	**If Yes, please list 3 recent clients:**
Individuals/Sole Proprietor Only **Government Employment:**	**Individual/Sole Proprietor** ☐ is ☐ is NOT a: ☐ CURRENT or ☐ FORMER employee of any U.S. Government entity or International Government entity **If yes, please specify:** **Current/Former Government Employer:** _____ **Separation Date (If Former):** _____	
Are you able to receive US Dollars (USD) through your bank?	☐ Yes ☐ No	

PAYMENT ADDRESS			AGREEMENT ADDRESS	☐ SAME AS REMIT ADDRESS	
Street Address:			**Street Address:**		
City:	**State:**	**Zip/Postal Code**	**City:**	**State:**	**Zip/Postal Code**
Country:			**Country:**		
Accounts Receivable Contact Name:	**Telephone No:**		**Contract Contact Name:**	**Telephone No:**	
Email Address:	**Fax No.:**		**Email Address:**	**Fax No.:**	

SUBCONTRACTOR/VENDOR BUSINESS SIZE CERTIFICATION

PRIMARY NAICS CODE FOR CERTIFICATION: enter primary NAICS https://www.sba.gov/size

This code will determine your default classification and is based on the type of work you are most likely to perform for EnCompass. If you do not know your primary NAICS, go to: http://www.census.gov/eos/www/naics/ to determine business size, contact your local SBA

☐ Small Business (SB)	☐ Service-Disabled Veteran-Owned SB	☐ 8A Certified Small Disadvantaged Business
☐ Large Business	☐ Foreign Owned Business	

❑ **Woman-Owned SB**	❑ **Small Disadvantaged Business**	❑ **Non-Profit**
❑ **Veteran Owned SB**	❑ **HUBZone SB**	❑ **Other** _____

By signature below, I hereby certify that the business type and designation indicated above is true and accurate as of the date of execution of this document, and I further understand that under 15 U.S.C. 645(d), any person who misrepresents a business' size status shall (1) be punished by a fine, imprisonment, or both; (2) be subject to administrative remedies; and (3) be ineligible for participation in programs conducted under the authority of the Small Business Act.

Signature and Title (required) Date

ENCOMPASS VENDOR QUESTIONNAIRE
Section 2

Fill in this form if 2 out of the following 3 are true:

1. The organization has not previously received USG funding (including but not limited to USAID, Department of State, Department of Defense, etc.)
2. The organization does not have an established Negotiated Indirect Cost Agreement (NICRA)
3. The organization is registered outside of the United States

If Supplier is owned or controlled by a common parent:					
Parent Name			Parent EIN		
Approximately how many employees do you currently employ?		Full-time		Part-time	
List all North American Industry Classification System Codes (NAICS) that apply to your company:					
http://www.census.gov/eos/www/naics/. To determine business size, contact your local SBA office https://www.sba.gov/content/find-local-sba-office;					

Financial Information

1. What are the beginning and ending dates of your organization's fiscal year?

From (month/day): _____ To (month/day): _____

2. What currency does your organization use to conduct its business activities?

_____

3. Please provide the following financial information based on your organization's most recent completed fiscal year.

Revenues: USD $ _____ Local Currency _____

Expenses: USD $ _____ Local Currency _____

Assets: USD $ _____ Local Currency _____

Liabilities: USD $ _____ Local Currency _____

Exchange rate: _____ = USD $1.00

4. Have you previously provided services on USAID-funded projects? Yes _____ No _____

If yes, please list up to three of your most recent projects, including project name, country, total contract value and if you were the subcontractor or prime contractor:

1. _____
2. _____
3. _____

5. Does your organization use indirect cost rates? Yes _____ No _____

If yes, please provide a copy of your indirect cost rate calculation.

6. Do you have a Negotiated Indirect Cost Rate Agreement (NICRA)? Yes _____ No _____

If yes, please provide a current copy.

Financial Control and Accounting System

1. How are your transactions recorded?

Manual ledger system – indicate ledgers used:

Computerized system – indicate software used:

2. Is there a chart of accounts? Yes _____ No _____

3. Is a double entry accounting system used? Yes _____ No _____

4. Does your organization have a written accounting policies and procedures manual?

Yes _____ No _____

If yes, please provide a copy.

5. On what basis are your financial reports issued? Cash: _____ Accrual _____

6. How often are financial reports prepared:

Monthly ____ Quarterly ____ Annually ____ Not prepared (please explain) _____

_____

7. Are timesheets used to record employees' total direct and indirect time charges?

Yes: _____ No _____

If yes, please attach a copy of the timesheet template.

8. Does your accounting system segregate direct costs from indirect costs?

Yes _____ No _____

9. Does your accounting system identify the receipt and expenditure of funds separately for each grant and/or contract?

Yes _____ No _____

10. Does the accounting system provide for the recording of grant/contract costs according to categories of the approved budget?

Yes _____ No _____

11. Are you familiar with the cost principles (Federal Acquisition Regulations Part 31.2, OMB Circular A-21, or A-122 as appropriate) and procedures for the determination and allowance of costs in connection with federal grants and contracts?

Yes _____ No _____

12. Is a separate bank account maintained for grant/contract funds?

Yes _____ No _____

13. If a separate account is not maintained, can the grant/contract funds and related expenses be readily identified?

Yes _____ No _____

14. Is your institution's accounting system designed to detect errors in a timely manner?

Yes ____ No ____

15. Are reconciliations between bank statements and accounting records performed monthly and reviewed by an appropriate individual?

Yes ____ No ____

Internal Controls

Internal controls are procedures which ensure that: 1) financial transactions are approved by an authorized individual and are consistent with U.S. laws, regulations and your institution's policies; 2) assets are maintained safely and controlled; and 3) accounting records are complete, accurate and maintained on a consistent basis. Please complete the following questions concerning your institution's internal controls.

1. Does your institution maintain a record of how much time employees spend on different projects or activities? If yes, how?

Yes _____ No _____

2. Do you maintain inventory records for your institution's equipment? If no, explain.

Yes _____ No _____

3. How often do you check actual inventory against inventory records?

4. Are all financial transactions approved by an appropriate official?

Yes _____ No _____

5. Is the person(s) responsible for approving transactions familiar with U.S. Federal Cost principles as described in Federal Acquisition Regulations Part 31.2, OMB Circular A-21, or A-122 as appropriate?

Yes _____ No _____

6. Does your institution use a payment voucher system or some other procedure for the documentation of approval by an appropriate official?

Yes _____ No _____

7. Does your institution require supporting documentation (such as original receipts) prior to payment for expenditures?

Yes _____ No _____

8. Does your institution require that such documentation be maintained over a period of time? If yes, how long are such records kept?

Yes _____ No _____

9. Are different individuals within your institution responsible for approving, disbursing, and accounting of transactions?

Yes _____ No _____

10. Are the functions of checking the accuracy of your accounts and the daily recording of accounting data performed by different individuals?

Yes _____ No _____

Audit

1. Is your organization audited on an annual basis? Yes _____ No _____

If yes, please attach a copy of the audited financial statements (including a Balance Sheet and Income Statement) for the last two fiscal years.

If no, has your organization ever been audited? _____

2. If you do not have a current audit of your financial statements, please provide this office with a copy of the following financial statements, if available:

- A Balance Sheet for the most current and previous year; and
- An Income Statement for the most current and previous year;
- A Cash Flow Statement for the most current and previous year.

3. Are there any circumstances that would prevent your institution from obtaining an audit?

Yes _____ No _____

If yes, please provide details:_____

Signed: _____
Name: _____
Title: _____
Date: _____