Request for Proposals

RFP-PSIA-2022-043

Activity Title: Power Sector Improvement Activity (PSIA)

Implemented by NUMARK Associates, Inc. and Energy & Security Group, LLC (ESG)

RFP Title: "Procurement, Installation, and Commissioning of Cyber Security System at PITC"

Request for Proposal (RFP) Timeline	
RFP Issue Date:	**June 9, 2022**
Questions Submission Deadline:	**June 20, 2022, at 5 pm Pakistan Time**
Proposal Submission Deadline:	**July 7, 2022, at 5 pm Pakistan Time**
Award Anticipated Date:	**August 2022**

Note: *Issuance of this RFP does not constitute an award commitment by NUMARK Associates, Inc, and Energy & Security Group, LLC (ESG). NUMARK Associates, Inc, and Energy & Security Group, LLC (ESG) will not pay for any costs incurred in preparation or submission of a proposal. Proposals are submitted at the risk of offerors. All preparation and submission costs are at the offeror's expense.*

ENERGY & SECURITY GROUP

TABLE OF CONTENTS

1. INTRODUCTION

The purpose of this RFP is to procure the supply, installation, and commissioning of a Cyber Security System for the Power Information Technology Company (PITC) in Pakistan. With cyberattacks becoming more frequent and sophisticated, the Cyber Security System will help PITC maintain a IT infrastructure in order to stay healthy and resilient against cyber threats. This multilayer cyber security platform will be commissioned as part of the work implemented by Energy & Security Group, LLC (ESG) under the Power Sector Improvement Activity (PSIA) Project funded by the U.S. Agency for International Development (USAID).

The PSIA project aims to support and facilitate Pakistan's transition to a competitive power market, while also improving operations of its transmission and distribution systems. The project will also optimize the use of its electrical grid through increased electrification which warrants a robust, secure, and efficient IT infrastructure. The PSIA project objectives are to focus on engaging the private sector as well as Pakistani and regional stakeholders and channel resources through the following three objectives:

Objective 1 – Increase power sector competition through support to develop Pakistan's wholesale electricity market:

The Government of Pakistan (GoP) has decided to introduce a competitive wholesale market in the power sector and PSIA plans to assist them in the operationalization of Pakistan's transition to a Competitive Trading Bilateral Contracts Market (CTBCM). The CTBCM will introduce competition in the electricity market and provide an enabling environment where multiple sellers and buyers can trade electricity directly with each other. To ensure that this transition takes place easily and effectively, PSIA will address existing processes, systems, policies, and codes that limit power sector advancements and will explore new concepts, such as energy wheeling (i.e., the transportation of electric energy from within an electrical grid to an electrical load outside grid boundaries), electricity auctions, expanding the power system's contractual flexibility, monitoring of the wholesale market, and creating a market for ancillary services. In addition, PSIA will also assist the GoP in establishing an open, transparent, and competitive procurement framework that will result in increased private sector investments in clean energy. These efforts will feed into the GoP's target of increasing Pakistan's share of renewables in its electricity generation mix to 60 percent by 2030.

Objective 2 – Improve the management and operation of transmission and distribution system:

Pakistan's short- and long-term energy security requirements call for improved management and operation of its transmission and distribution companies. To improve the performance of these transmission and distribution companies, PSIA will work with these entities to increase their technical and operational capacity by developing and conducting training for company staff, providing tools and resources to improve their performance, and providing IT and other technical support. Additionally, PSIA will also propose innovative and proven solutions to improve power system operations—such as integration of renewable energy—that aligns with global trends away from fossil fuel-based technologies. These solutions will help reduce carbon and other harmful emissions while also enhancing Pakistan's energy forecasting and planning capabilities. Additionally, PSIA's proposed solutions will help increase customer satisfaction, improve sector revenues, and better accommodate anticipated technological changes in power generation, transmission, and distribution (e.g., through grid modernization investments).

Objective 3 – Optimize Grid Electricity Load

Seasonal variations in demand significantly impact grid loads as people use more electricity in the hot summer months compared to the cold winter season, leading to idle generation plants that still require high-capacity charges. This contributes to increasing the sector's 'circular debt' and, eventually, consumer tariffs. To optimize grid electricity loads, PSIA will introduce systems, procedures, and new end-uses in the transportation, industrial, commercial, and residential sectors that consume electricity more efficiently and productively, reducing primary energy inputs and increasing revenues and incomes. PSIA support will also be provided to improve grid stability and supply quality, especially in weak grid areas. Additionally, PSIA will devise solutions to incentivize increased electrification of the economy (e.g., electric vehicles and displacement of gas-fired equipment.) that can help improve national productivity and quality of life, while reducing fuel imports and harmful emissions.

2. OFFEROR QUALIFICATIONS

Offerors must provide the following information and references to qualify for award:

1. **Company information**, including official registered name, place of legal registration of the business, type of business, address, and identity of principal company officers. If the company has more than one office, please indicate which location is proposed to lead implementation.
2. **A brief description of the company and its experience** providing identical or similar services to those described in the Technical Specifications.
3. **Completed and signed representations and certifications** found in Attachment C.

3. SUBMISSION OF PROPOSALS

Proposals are due **July 7, 2022, at 5 pm local time in Islamabad, Pakistan.** Proposals must be sent to RFP@energyandsecurity.com. The subject line must include "Company Name-RFP-PSIA-2022-043." Late proposals will not be considered**. It is the offeror's responsibility to ensure receipt, which will be acknowledged upon request.**

All proposals must fully respond to the scope of work in **Attachment A** and must include a financial offer in the format prescribed in **Attachment B**. The financial offer must be sent as a separate document.

Proposals should not contain any unnecessary promotional material.

Offerors must follow all instructions to be qualified for award. Offeror Proposals with material deviations from any administrative and/or technical requirements may not be considered. Proposals with non-material deviations may be downgraded and not receive full credit under the applicable evaluation criteria.

A. TRANSMITTAL LETTER

A transmittal letter on the Offeror's company letterhead must certify that prices are accurate, complete, current, and valid for at least 90 days.

B. OFFEROR INFORMATION

1. Company description that illustrates overall product line and corporate capability to meet all terms of this RFP.
2. Organization information, including official registered name, place of registration, type of business, list of principal company officers, company address, telephone number, and website address.
3. Authorized point of contact and company officer(s) authorized to sign an award with phone number(s) and email address(s).
4. For Offerors located outside of Pakistan, contact information of the authorized local representative.
5. Past Performance Information – Company's past similar experience within the last two years performing work in Pakistan or in locations not included in the US Department of the Treasury Office of Foreign Assets Control (OFAC) country sanctions list. Offerors shall include at least two past performance citations of successful performance of similar requirements including: equipment and services provided, date of delivery, quantity, client contact information, and any additional information that may assist in certifying performance. Experience of the offeror's principal representative delivering requirements may also be considered. Past performance references are limited to a maximum of five of the most relevant contracts performed in the last five years, presented in the format below. If the client is confidential, please indicate "confidential."

Title of Contract	Description of the Contract	Client Name	Dates of Execution	Contract Value $

6. Offeror's Unique Entity Identifier number, if proposed price is more than USD $30,000 or PKR equivalent (Please see Section 12 below for information on the UNIQUE ENTITY IDENTIFIER NUMBER).
7. The Offeror must disclose in writing with its offer any subcontracting that will take place under an award. Failure to disclose subcontracting relationships will result in the prospective Offeror being removed from consideration.

C. COMPLIANCE WITH TECHNICAL AND FUNCTIONAL SPECIFICATIONS

Offerors are required to review and confirm specifications for each equipment component and complete the table below which compares the proposed specifications to the specifications requested in this RFP. Offerors should respond using plain language that is concise, unambiguous, quantitative, and complete. Offerors may volunteer additional information if

directly relevant. Please use the table provided below to explain adherence to or deviations from specifications.

Requested Specifications	Proposed Specifications	Complied Yes or No	Notes

D. DELIVERY PLAN

Offerors are required to meet the required delivery schedule of 90 days from the date of award. Offerors must also provide a detailed schedule specifying dispatch, delivery, and installation at PITC HQ WAPDA House Lahore, Pakistan.

E. SUPPORT SERVICES

A description is required of how Offerors will support the required and offered products. Support Services are an important consideration in selecting suppliers for USAID-funded projects. **Energy & Security Group, LLC (ESG) requires a commitment to provide follow-on support in Pakistan during the minimum warranty period of three years from the date of installation and commissioning.**

Procurement support will include:

- Ongoing technical assistance.
- Hardware Warranty Service - Offerors must provide information on hardware warranty and availability of services in Pakistan for a minimum period of three years. Offerors must indicate the extent of the coverage to include services, product replacement, and other applicable factors.
- Software License – All software licenses shall be valid for a minimum period of three years from the date of installation.
- Offerors must provide an original equipment manufacturers' (OEM) warranty with the proposal. All warranties and software licenses shall be in the name of PITC. Offerors must also provide PITC with all relevant documentation to enable it to enforce warranties.
- Provide name and address of the authorized service facility in Pakistan.

F. REPRESENTATIONS AND CERTIFICATIONS

Offerors must provide the representations and certifications found at Attachment C.

G. PRICE PROPOSAL

Offerors must submit a detailed budget of all prices in identified cost lines that present comprehensive prices of equipment and all other costs separately in electronic form. Offerors must provide quotations for all items as a part of complete solution. PSIA will not accept lump-sum totals for categories. Offerors are encouraged to choose the technical components from sources that will provide the least expensive and best available mix of equipment. Offerors may provide different equipment source options (see RFP section 6 below) so that Energy & Security Group, LLC (ESG) may evaluate the total cost offered based on shipping from different locations, as long as these are within the USAID Authorized Geographic Code (937).

Price Proposals must show unit prices, quantities, and total price. All equipment and services must be clearly identified and included in total offered prices. Proposals must include a budget narrative that explains the basis for the estimate of every cost element or line item. Supporting information must be provided in enough detail to allow for a complete evaluation of each cost element or line item. Energy & Security Group, LLC (ESG) reserves the right to request additional information.

Payments will be linked to the proposed deliverables. Energy & Security Group, LLC (ESG) intends to issue a Firm-Fixed-Priced subcontract or purchase order. Payment will be made upon delivery and acceptance of each item by the ESG Chief of Party or assigned technical representative.

Prices quoted must be valid for at least 90 days and include all taxes and VAT and costs of doing business. Any taxes and VAT that will be applicable to this procurement must be shown as a separate line item(s) in order to facilitate required reporting.

The cost of, and requirements to, obtain compliance certificates from the equipment testing agencies and the Government of Pakistan are the sole responsibility of the successful offeror.

Financial Offer: Offerors must provide a price offer for delivery, installation, testing, and commissioning of finished products/systems (goods) at PITC Lahore, Pakistan. Offerors should also budget for all applicable taxes such as VAT**,** General Sales, and other applicable Taxes. Government approval certification costs and local shipment costs to the destinations must be shown as a separate line item(s).

Successful Pakistani offerors will be paid in PKR by the PSIA Islamabad Office based on the US $ exchange rate published by the State Bank of Pakistan on the day of invoice payment. All of the above or any other charges and applicable taxes should be budgeted as separate budget line items in the price proposal.

Energy & Security Group, LLC (ESG) reserves the right to conduct discussions with offerors to determine compliance with the RFP requirements and to determine the offer representing the best value.

Price information must not be included in the technical proposal. All cost and pricing information must only be shown in the cost proposal.

4. QUESTIONS AND CLARIFICATIONS

Questions and requests for clarifications must be in writing and submitted in the English language to RFP@energyandsecurity.com by **June 20, 2022, at 5 pm Pakistan Standard Time.** All questions and responses will be distributed to all RFP recipients. Please include the RFP number in the subject line of emailed questions.

No phone calls or other verbal questions will be acknowledged.

All those who receive the RFP are encouraged to inform PSIA at the email address above, so that PSIA can ensure that all interested parties receive the Questions/Answers and any amendments which may be issued.

5. SOURCE AND NATIONALITY RESTRICTIONS

The authorized geographic code for this RFP is Code 937, which is defined as the **United States, Pakistan, and developing countries *other* than advanced developing countries.** This means that all Nationality of Suppliers (Offerors) must meet the authorized geographic code and that the Source of all commodities and services supplied must also be compliant with the geographic code.

All requirements under any award resulting from this RFP must meet this geographic code in accordance with the US Code of Federal Regulations (CFR), 22 CFR 228.

A list of Advanced Developing Countries is located at http://www.usaid.gov/sites/default/files/documents/1876/310mab.pdf.

6. REPRESENTATIONS AND CERTIFICATIONS

Offerors must complete and sign the Representations and Certifications form in Attachment C. Proposals that do not include these signed certifications will not be considered for award.

7. EVALUATION

Award will be made to the offeror(s) whose proposal is determined responsive to this solicitation document, meet all eligibility criteria, meet technical and corporate capability requirements, and is evaluated as the best value offer to ESG and the PSIA.

ESG intends to evaluate proposals in accordance with this section and to make an award to the responsible Offeror(s) whose proposal(s) represents the best value. "Best value" is defined as the offer that results in the most advantageous solution for the Project, in consideration of technical, cost, and other factors.

The submitted technical proposal will be scored by a Technical Evaluation Committee (TEC) using the technical criteria outlined below. When evaluating the competing Offerors, ESG will consider the written qualifications and capability information provided by the Offerors, and any other information obtained through its own research.

All evaluation factors other than cost/price when combined are significantly more important than cost/price.

Proposals will be evaluated and scored against the evaluation criteria in the table below. Proposals will be scored by an evaluation committee on a 100-point scale.

Energy & Security Group, LLC (ESG) reserves the right to conduct discussions with selected offerors. ESG may request a presentation/demonstration to assess compliance to technical qualifications.

ESG may send inquiries to the clients of offerors and may obtain information related to projects that offerors have performed. ESG may request clarifications or additional information and reserves the right to make an award decision based solely on the information provided with the proposal. ESG may conduct negotiations prior to award and may at its sole discretion elect to issue subcontracts/orders to one or more offerors.

The Cost Proposal will not be scored but it will be evaluated. Cost will primarily be evaluated for realism, reasonableness, allowability, consistency with current market rates, and overall cost. This evaluation consists of a review of the cost portion of an Offeror's proposal to determine if the overall costs proposed are realistic for the work to be performed, if the costs reflect the Offeror's understanding of the requirements, and if the costs are consistent with the Technical Proposal and the efficient use of funding. Proposal prices may be adjusted to include all charges such as annual service, licensing charges (if any), warrantee charges for three years, and installation and commissioning charges.

Technical evaluation criteria are:

EVALUATION CRITERIA (IN DESCENDING ORDER OF IMPORTANCE)

Evaluation Criteria -
a. Compliance with technical and functional specifications/requirements
b. Delivery and installation schedule
c. **Company profile and past performance**
d. Capacity/capability of providing after sales services and support

8. NEGOTIATIONS

Best offer proposals are requested. However, ESG reserves the right to conduct discussions, negotiations, and request clarifications prior to awarding a subcontract. Furthermore, ESG reserves the right to conduct a competitive range competition and to limit the number of proposals in the competitive range to permit an efficient evaluation among the most highly rated proposals. Offerors submitting the highest-rated proposals may be asked to submit revised best prices or technical responses during a competitive range. At the sole discretion of ESG, offerors may be requested to conduct oral or other presentations.

9. GENERAL TERMS AND CONDITIONS

Energy & Security Group, LLC (ESG) intends to award firm-fixed-price subcontract(s)/purchase order(s) resulting from this solicitation to the responsible offeror(s) whose proposal(s) is considered to represent the best value. Offerors should note the following:

- ESG reserves the right to increase or decrease the quantity up to 30 percent of original quantities at the agreed price at the time of award or issue a subsequent order at the same price up to 30 percent of original quantity during the currency of the subcontract resulting from this solicitation under the same terms and conditions.
- ESG reserves the right to evaluate proposals and award contract(s) without discussions with offerors (except clarifications as described in FAR 15.306(a)). Therefore, the offeror's initial proposal should contain the offeror's best terms from a cost or price and technical standpoint. ESG reserves the right to conduct discussions and/or to establish a competitive range and conduct discussions with multiple offerors if ESG later determines discussions to be necessary.
- Unsuccessful offerors will be notified as soon as possible following an award.
- ESG reserves the right to perform pre-delivery inspections on all equipment to verify the compliance to the technical specifications and validate quality control and ISO standards as defined in terms and conditions of the subcontract/order.
- In the event the subcontractor fails to complete the project within the required period, liquidated damages will be applied for each calendar day, not duly justified by the subcontractor by which project delivery is delayed. Liquidated damages of one-half percent (0.5 percent) of the total price of the subcontract will be applied for each day by which delivery is delayed. Such damages shall not exceed 20 percent of the total price of the subcontract.
- ESG reserves the right to monitor the subcontractor’s progress to ensure it meets the implementation milestones as determined at the time of award. If it appears that a milestone will be missed, a cure letter will be issued to the subcontractor which may order subcontractor to field more teams or increase the number and qualifications of staff to remain within project

timelines – at no additional cost to ESG. Continued missing of timelines may lead to contract termination and/or penalties.

- ESG will monitor the quality of work performed by the subcontractor. If the quality of work is inadequate, ESG reserves the right to order the subcontractor to reperform work judged to be of insufficient quality.
- ESG may determine that a proposal is unacceptable if the prices proposed are materially unbalanced between line items or sub-line items. Unbalanced pricing exists when, despite an acceptable total evaluated price, the price of one or more contract line items is significantly overstated or understated as indicated by the application of cost or price analysis techniques. A proposal may be rejected if ESG determines that the lack of balance poses an unacceptable risk.
- **All goods proposed must be new, unused, not rebuilt or reconditioned, and shall not incorporate reconditioned or salvaged parts or components.**
- ESG may, in its sole discretion, reject any or all proposals without assigning any reason and without thereby incurring any liability to a prospective offeror or to any other person.
- ESG may, in its sole discretion, withdraw, annul, suspend, or cancel the RFP or the bidding process without incurring any liability to a prospective offeror or to any other person.
- Proposals will be held as confidential, will not be disclosed outside of ESG, and will not be duplicated, used, or disclosed-in whole or in part-for any purpose other than evaluation for potential subcontract award. If, however, a subcontract is awarded as a result of submission of a proposal, ESG will have the right to duplicate, use, or disclose the data contained therein to the extent provided in the resulting subcontract. This restriction does not limit ESG's right to use information contained in a proposal if it is obtained from another source without restriction.

10. PERIOD AND PLACE OF PERFORMANCE

The period of performance for this award will be up to 90 days from date of award. The place of performance will be in PITC Lahore, Pakistan.

11. TERMS OF PAYMENT

Payment terms are net 45 days after submission of proper invoices for work satisfactorily performed and accepted. Payment shall be made by ESG via check or wire transfer or through its Islamabad Office if the subcontractor is based in Pakistan. Should a subcontract be awarded to a Pakistani firm, all payments will be made in Pak Rupees based on the US $ exchange rate published by the State Bank of Pakistan on the day ESG is making the payment to the subcontractor. A payment schedule with required deliverables will be established in the subcontract. **No advance payments will be provided.**

The Power System Improvement Activity (PSIA) Project implemented by NUMARK Associates, Inc., and Energy & Security Group, LLC (ESG) is exempt from General Sales Tax (GST) in accordance with a bi-lateral agreement between the United States and Pakistan (1951 Technical Cooperation Treaty and the 2010 Pakistan Enhanced Partnership Agreement) and as such is entitled to a refund of any GST paid to any entity providing goods and services under USAID funded programs upon presentation by ESG of a certification of exemption received from an authorized authority from the Government of Pakistan.

Tentative Payments Schedule for the cyber security system hardware and necessary software will be made in two stages and the actual payments schedule is subject to negotiation and mutual agreement:

1. Subcontractor will be paid 60 percent of the total value of the hardware and accessories, including cost, freight, and insurance, shipped to the project site upon receipt of the following documentation after all terms and conditions of the Agreement have been fulfilled:

    a) Proper invoice specifying the items, including the manufacturer and catalog number of each; and the unit prices, quantities, and total value of the items for which payment is requested.

    b) Packing list for the materials showing the number of packages and their contents.

    c) Original freighted Bill of Lading for the materials evidencing embarkation of the goods to the Destination.

    d) A copy of the invoice evidencing payment of shipping and insurance costs.

    e) For imported goods, a Certificate of Insurance demonstrating the acquisition of all-risk shipping insurance to the destination in the amount of 110 percent of the total value of the materials

    f) Certificates of Origin for all materials.

    g) OEM (Original Equipment Manufacturer) Certificate.

    h) Inspection and material acceptance certificate issued by the PSIA Project Manager or designee based on system acceptance by PITC.

2. Balance payment will be made after successful installation, commissioning, operation, and acceptance by PSIA and PITC.

12. UNIQUE ENTITY IDENTIFIER

If the proposed price is above the PKR equivalent of USD $30,000, the successful offeror will be required to furnish a Unique Entity Identifier number within two business days of notice of award. Information regarding obtaining a Unique Entity Identifier number may be found at www.sam.gov. Offerors are encouraged to begin the application process early.

13. MULTIPLE AWARD/NO AWARD

ESG reserves the right to issue multiple awards. ESG also reserves the right to issue no awards.

Issuance of this RFP does not constitute an award commitment on the part of ESG and ESG will NOT pay for costs incurred in the preparation and submission of proposals.

Note: ESG has zero tolerance for fraud. Fraud is any act or omission that intentionally misleads, or attempts to mislead, to obtain a benefit or to avoid an obligation. If you have concerns about potential fraud in any way related to ESG projects, contracts, or activities, please contact ESG's Ethics Officer at **katsalinos@energyandsecurity.com** or at (703) 476-3207.

ATTACHMENT A: TECHNICAL AND FUNCTIONAL SPECIFICATIONS

SCOPE OF WORK:

Procurement, Installation, and Commissioning of Cyber Security System at Power Information Technology Company (PITC)

PERIOD OF PERFORMANCE: 90 days from date of award
PLACE OF PERFORMANCE: Lahore, Pakistan

A.1 SCOPE OF WORK

The scope of this RFP includes the supply, installation, and commissioning of Cyber Security System including Hardware and Software and other services as specified below. This solicitation of Cyber Security System and associated hardware/software is intended to be used by Power Information Technology Company (PITC) in Pakistan. All charges related to supply, testing, material inspection, transportation, installation hardware, and any other related costs shall be borne by the offeror. Hence the prices quoted shall be inclusive of all such charges.

A.2 FUNCTIONAL SPECIFICATIONS AND REQUIREMENTS

A.2.1 END-USER SECURITY REQUIREMENTS

a. General Requirements

i. Solution must accommodate minimum 1,000 users

ii. Solution must have option for hybrid deployment (on premise and cloud management server)

iii. Solution must integrate with Active Directory in case of hybrid deployment

iv. Solution must include web-based administration for on premise and cloud management server

v. Solution should have centralized security management with a web and cloud console

b. Threat Protection

i. Solution must include signature-based detection with behavior monitoring through machine learning (ML).

ii. Solution must have technologies to detect, stop, and restore encrypted files from ransomware.

iii. Solution shall have ML-driven threat protection that is effective even without regular updates.

iv. Solution shall provide pre-execution detection and blocking of new and evolving threats (advanced ML and suspicious file behavioral monitoring and blocking), and signature-based methods.

v. Solution shall have system watcher or behavior analysis to protect against file-encrypting malware and rolls back the changes made by malicious applications.

vi. Solution shall have exploit prevention feature that denies attackers by blocking the exploit tools and techniques used to distribute malware, steal credentials, and escape detection.

vii. Solution must include web protection to prevent access to malicious websites.

viii. Solution must include host-based firewall.

ix. Solution must include host-based intrusion prevention system (IPS).

x. Solution must provide an application to implement blacklisting or whitelisting or lock-down.

xi. Solution must be able to provide sandbox integration, preferably cloud-based sandbox.

xii. Sandbox integration with endpoint shall be included in offering.

c. Sandbox

i. Sandbox should be on premises with the ability to analyze minimum 30K files per day. It must have the ability to create customized sandbox images for virtual execution based on PSX environment in order to effectively detect targeted attacks.

ii. Solution must not be detectable by malware in order to avoid evasion. The solution must be able to detect when system sleep functions are used by malware to evade detection and must be able to accelerate the time to force the malware into execution. The solution must be able to simulate end-user actions in order to force the execution of malware that rely on triggers from and end user, like a mouse click.

iii. Solution must be able to utilize a live internet connection to better understand the malware analyzed. It must also be able to utilize a separate network interface for the live communication and not the management interface.

iv. Solution must support the following Windows operating systems for sandbox: Windows 7, Windows 8/8.1, Windows 10, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, Linux at minimum.

d. Device Control

i. Solution must be able to restrict device access on endpoints by assigning rights to read, read/write, write, and deny access to USB drives.

ii. Solution must have option to allow organization's approved mass storage/USBs.

iii. The device control feature must also provide restriction for the following:

- CD-ROM
- Network Shares

e. Endpoint Data Encryption

i. Solution must provide endpoint encryption for full disk and file/folders.

ii. Solution must provide encryption for USB devices.

iii. Solution must also provide management for BitLocker.

iv. Solution must offer remote wipe of laptops.

f. Mobile Security

i. Solution must provide mobile device management features including:
   - Device provisioning
   - Policy control and management
   - Software management

ii. Solution must provide mobile data protection features such as:
   - Encryption enforcement
   - Remote wipe
   - Remote lock
   - Selective wipe

iii. Solution must provide mobile device security features such as:
   - Anti-malware capability
   - Rooted device detection
   - Detects and blocks malicious applications and data files
   - Blocks malicious web content and sites
   - Must provide support for both Android and iOS devices

g. Endpoint Detection and Response

i. The proposed Solution must support 1,000 users

ii. Solution must have endpoint, detection, and response (EDR) capability that allows for the monitoring, recording, and performing of both current and historical security investigations and should help in assessing the extent of damage.

iii. Solution should allow users to drill down on an interactive process tree that illustrates the full chain of attack in order to identify how the detection was able to arrive, what changes were made, and how it was spread by analyzing activities performed by objects and processes.

iv. Solution must have the ability to provide immediate response in order to terminate processes or isolate users or update security. In addition, users should also have the ability to use current findings to sweep more endpoints.

v. Solution must allow users to sweep endpoints with multiple search parameters. Sweeping must be available on parameters such as communication being done, file hashes, registry-based activity, user activity, and running processes.

vi. Solution must also support industry standard Open IOC or YARA rules.

h. Email Security

i. The proposed Solution must support 1,000 users

ii. Solution must be leader in Forester Wave Email Security report.

iii. Solution must be Hardware (HW) appliance.

iv. Solution must have integrated Sandbox in same HW appliance.

v. Solution must act as simple mail transfer protocol (SMTP) relay/message transfer agent (MTA) and must include spam filtering engine, IP reputation/real-time blackhole list (RBL) feature, sender policy framework (SPF), DomainKeys Identified Mail (DKIM) and DMARC feature and should provide marketing/graymail filter.

vi. Solution should be able to offer following settings for proper SMTP relay/MTA configuration:

- Message delivery
- Configuring SMTP connection settings
- Configuring message delivery settings
- Configuring limits and exceptions
- Configuring the SMTP greeting message
- Edge MTA relay servers

vii. Solution should provide and end-user quarantine feature to improve spam management. Messages that are determined to be spam should be available for users to review, delete, or approve for delivery. The solution should be able to automatically send digest notifications to end-users.

viii. Solution must be able to detect known and unknown or targeted attacks with sandbox analysis.

ix. Solution must have sandbox with customization capability and sandbox must support Windows,7,10, Server 2008,2012, 2016, and 2019

x. Solution must have capability to import Yara rules.

xi. Solution must analyze URL in sandbox and corresponding payloads downloaded from that URL.

xii. Solution must share Threat Intelligence with other vendors solutions.

xiii. Solution must include machine learning feature to detect malware and must have URL reputation feature to detect phishing or malware-based URLs. Additionally, the solution must be able to analyze URLs in sandbox as well and provide complete report on any suspicious objects identified. The solution should also provide URL time-of-click protection.

xiv. Solution must have capability to check URLs in email subject.

xv. Solution should be able to detect social engineering attacks by analyzing several parts of email transmission including email header, subject line, body, attachments, and SMTP protocol information.

xvi. Solution must be able to detect fraud/business email compromise attacks and it should be possible to select specific high-profile users to detect possible fraud/business email compromise attack to them.

xvii. Solution must provide high level view of threat monitoring via dashboard including:

- Attack sources widget
- High-risk messages widget
- Detected messages widget

- Advanced threat indicators

xviii. Solution must provide high level view of system status via dashboard:

- Processing volume widget
- Hardware status widget

xix. Solution must provide high-level view of top trends via dashboard:

- Top attachment names widget
- Top attachment types widget
- Top affected recipients widget
- Top attack sources widget
- Top callback hosts from sandbox widget
- Top callback URLs from sandbox widget
- Top Email Subjects Widget

xx. Solution should provide ability to generate reports for the following frequency:

- Daily
- Weekly
- Monthly

xxi. Solution should provide at-least the following logs:

- Email message tracking
- MTA events
- System events
- Message queue logs
- Email submission logs
- Time-of-click protection logs

xxii. Solution must utilize multiple detection engines and sandbox simulation to investigate file attachments. Supported file types must include a wide range of executables such as Microsoft Office, PDF, web content, and compressed files. Sandbox environment must detonate files, including password-protected archives and document files, and URLs to test for malicious behavior.

xxiii. Solution must be able to detect threats hidden in password-protected files and password-protected archives and should be able to detect threats masqueraded in shortened URLs.

xxiv. Solution should be able to take action on suspicious email messages such as block, quarantine, and delete and should have the capability to whitelist certain email messages to pass through to the recipient. The solution should also be capable to strip suspicious attachments, redirect suspicious links to blocking or warning pages, and tag the email subject with a customized string. The solution should notify recipients when a policy rule is matched and must be able to send copies of malicious detected email messages to archive servers.

xxv. Solution should be able to effectively block content that is specified as inappropriate from reaching recipients by analyzing both the message content and attachments. The proposed solution should also be able to prevent sensitive content being sent outside by analyzing message content and attachments.

xxvi. Solution should have data loss prevention (DLP) templates for data leakage over email.

xxvii. Solution must have an option to direct email sample analysis with manual email submission on proposed product's Web user interface (UI).

xxviii. Solution must detect phishing, spam, Business Email Compromise (BEC) scams, graymail, and social engineering attacks.

xxix. Business Email Compromise protection must have content inspection including email Intention Analysis. The content of the email is examined for a sense of urgency, a request for action, or a financial implication.

xxx. Solution must have email authorship analysis feature, by using artificial intelligence (AI) to determine if the email is impersonating a high-profile user by examining the writing style.

xxxi. Solution must provide the ability to examine the message contents to determine whether the message contains inappropriate content.

i. Security for MS Exchange

i. Solution must support 1,000 users.

ii. Solution be installed on MS Exchange Server and able to scan internal emails for hateful content.

iii. Solution must support Exchange Server 2013, 2016, and 2019.

iv. Solution must support SMTP scanning.

v. Solution must detect and take action against viruses/malware, Trojans, and worms.

vi. Solution must detect and take action against spyware.

vii. Solution must support file type recognition to detect falsely labelled files.

viii. Solution must detect document exploits and other threats used in advanced attacks.

ix. Solution must support scanning for mailbox.

x. Solution must support content filtering rules.

xi. Solution must support data loss prevention to block sensitive data.

xii. Solution must provide anti-spam capability.

xiii. Solution must provide Click-Time Protection for URLs.

xiv. Solution must include a search and delete feature to delete unwanted email or content from email.

xv. Solution must have DLP to stop confidential emails.

j. Data Leakage Prevention Control

i. The proposed Solution must support 1,001 users.

ii. Solution should have data discovery capability on endpoints.

iii. Solution should protect against data leaks via USB drives and other channels based on specified sensitive content.

iv. Solution should be able to stop data leakage on Web and email.

v. Solution must have capability to protect data on keywords.

vi. Solution must have capability to protect data on expressions.

vii. Solution must have capability to protect data based on file type.

viii. Solution must support user justification option when violating the DLP policies.

ix. Solution must have capability to block print-screen function.

k. Web Gateway Security

i. The proposed Solution must support 1,000 users.

ii. Solution must include cloud proxy for roaming users and on-premises software appliance for local enterprise users with centralized cloud management.

iii. Solution should provide multi-layered gateway-level protection against the latest web-based threats.

iv. Solution should block infections before they can reach your endpoints.

v. Solution must allow protection of both iOS-based and Android-based mobile devices.

vi. Solution must monitor and analyze web traffic status and network threats by using the dashboard, log, and report features.

vii. Solution must assign suitable bandwidth resources for critical traffic to control communications.

viii. Solution must decrypt and inspect encrypted content and manage digital certificates by using the HTTPS inspection feature.

ix. Solution must integrate with popular search engines and online services, such as Bing and YouTube, to leverage their Search Safety feature.

x. Solution must facilitate a more user-friendly experience by providing multiple types of event notifications, alerts, and messages to users and administrators.

xi. Solution must support dynamic URL categorization technology to perform real time categorization of the website based on the website content and HTTP URL.

xii. Solution must provide machine learning feature for unknown malware detection.

xiii. Solution must support authentication with on-premises AD, Microsoft Azure AD, Okta and ADFS.

xiv. Solution shall detect advanced attacks and provide an automated response.

A.2.2 SERVER SECURITY REQUIREMENT

a. General Requirements

i. Solution must support 125 Servers

ii. Solution must provide single dashboard for physical, virtual, and cloud servers.

iii. Solution must have support for Windows, Linux, AIX, and Solaris operating systems.

iv. Solution must provide IPS for Windows and Linux.

v. Solution must provide IPS for AIX and Solaris.

vi. Solution must have support for Server Windows 2003, 2008, 2012,2016, and later.

vii. Solution shall provide layered defense against advanced attacks and provide shield against vulnerabilities on OS level and application level.

viii. Solution should be able to provide security shield against WebSphere Application Server vulnerabilities.

ix. Solution should be able to provide security shield against Oracle Web Logic.

x. Solution should be able to identify use of PSEXEC tool through SMB share.

xi. Solution should be able to detect and alert if executable file is being uploaded on a SMB share.

xii. Solution should be able to detect and alert batch file upload on network share.

xiii. Solution should be able to identify and alert on suspicious (RDP) possible attempt of brute force.

xiv. Solution should be able to prevent access to administration share.

xv. Solution should be able to detect OneDrive, Dropbox, BOX traffic.

xvi. Solution should be able to detect download of a file over FTP.

xvii. Solution should be able to detect traffic remote applications like VNC and TeamViewer.

xviii. Solution must provide firewall feature on Windows, Linux, and AIX.

xix. Solution must have application control feature to quickly identify new suspicious files.

xx. Solution must provide IPS feature on Windows, Redhat, and AIX.

xxi. Solution must be able to detect and alert on administrator log-ins on servers.

xxii. Solution must be able to alert when log file is cleared (e.g., Windows Event Logs).

xxiii. Solution must be able to detect PowerShell command execution.

xxiv. Solution shall be able to detect ftpd events on Solaris.

xxv. Solution shall be able to detect ftpd events on AIX.

xxvi. Solution shall be able to detect ftp event on Windows.

xxvii. Solution shall be able to detect hosts file modification on Windows.

xxviii. Solution shall be able to detect file attribute changes in /usr/bin and /user/sbin on Unix.

xxix. Solution shall be able to detect change in the attribute Permissions of any log file under /var/log path.

xxx. Solution shall be able to alert when command history is cleared.

xxxi. Solution shall be able to detect installation of root certificate.

xxxii. Solution shall be able to detect removable devices on Linux.

xxxiii. Solution shall be able to identify create and delete activity of users and groups.

xxxiv. Solution shall be able to detect when task scheduler entries are modified.

xxxv. Solution shall be able to detect when Windows start up programs are modified.

xxxvi. Solution shall be able to detect when a software is installed or uninstalled on Unix.

xxxvii. Solution shall be able to detect files created by Oracle Bea WebLogic Server when modified.

xxxviii. Solution shall be able to provide lock-down ability (to block all new executable) if needed on Linux.

xxxix. Solution shall be able to provide information on the user and process associated with launching of executable.

xl. Solution shall be able to provide a way to block suspicious list of hashes on Linux.

xli. Solution shall be able to list down the vulnerabilities being protected with relevant CVE and CVSS score.

xlii. Solution shall be able to provide a mechanism to block suspicious web traffic.

A.2.3 NETWORK SECURITY

a. Network Anti-APT Solution

i. Solution must come with hardware appliance.

ii. Security vendor should have a platform to address both advanced persistent threat (APT) and advanced malware across network proactively.

iii. Solution should have behavior detection capabilities and analyzes traffic and objects.

iv. Current requirement is to inspect up-to 1G of traffic irrespective of number of users involved.

v. Solution must support 90+ protocols including SMB for lateral movement detection. Share list of all protocols.

vi. Solution must be able to detect and report malware downloaded.

vii. Sandbox solution must not be detectable by malware in order to avoid evasion.

viii. Solution must have ability to detect when system sleep functions are used by malware to evade detection and must be able to accelerate the time to force the malware into execution.

ix. Solution must have ability to simulate end user actions in order to force the execution of malware that rely on triggers from and end user, like a mouse click.

x. Solution must provide the full detailed malware analysis report for the malware executed in sandbox.

xi. Solution should perform dynamic real-time analysis of advanced malware on the appliance itself to confirm true zero-day and targeted attacks.

xii. Solution should provide network exploit detection.

xiii. Solution should provide document exploit detection.

xiv. Solution should provide feature to analyze scripts.

xv. Solution should be able to handle evasion tactics (Anti-VM, Anti-Sandboxing, and Anti-Debugging).

xvi. Solution should have the ability to remain completely invisible to both the end user as well as the attacking website.

xvii. Solution should be able to detect rootkits.

xviii. Solution should be able to handle DLL injections.

xix. Solution must be able to accurately identify malware and maintain a very low false-positive rate.

xx. Solution must be able to utilize XFF headers to identify the client machine generating the alerts when deployed in front of a proxy server.

xxi. Solution must allow the administrator to associate file extensions to the applications that will run the files in the sandbox.

xxii. Solution should have the ability to display the geo-location of the remote command and control server(s) when possible.

xxiii. Solution should have the ability to report the Source, Destination, Detection Name, Detection Severity and Protocol.

xxiv. Solution should detect potential malicious network traffic, such as DNS queries to Botnet C&Cs.

xxv. Solution should monitor SMTP Traffic.

xxvi. Solution should be able to integrate with investigation platform to perform threat hunting and investigation.

b. Next Generation Intrusion Prevention Systems

i. For remote sites, the throughput required is 1Gbps in HA.

ii. Solution must provide “dedicated” and “stand-alone” next-generation IPS functionality.

iii. Solution must also be able to act in IDS mode via span traffic.

iv. Solution must be able to prevent against vulnerabilities that are not yet disclosed.

v. Solution must have weekly signatures update for "unknown or undisclosed attacks" that do not yet have common vulnerabilities and exposures (CVE).

vi. Solution must provide on-box SSL inspection for both inbound and outbound traffic.

vii. Solution must provide machine learning ability to detect evolving security threats.

viii. Solution must provide real-time threat detection and mitigation based on statistical models.

ix. Solution must have integration with sandbox. This feature is not required right now but is needed for future consideration.

x. Solution must be able to inspect asymmetric traffic.

xi. IPS must be able to use reputation service such as IP address or DNS to block traffic from or to 'known bad host' such as spyware, phishing, or Botnet C&C.

xii. IPS appliances must be managed via a centralized management system.

xiii. The management system solution must be available in high capacity in the event one appliance goes down, the other one should be able to take the management burden.

xiv. All proposed IPS appliances' configuration, software updates, profile distribution, and rule filters should be managed via the centralized management system.

xv. Solution must use a combination of technologies, including deep packet inspection, threat reputation, and URL reputation to detect and prevent attacks on the network.

xvi. IPS appliances must support flexible licensing for future-proofing the expansion requirements with the same appliances.

xvii. Solution must support administrator authentication via RADIUS, LDAP and TACACS+

xviii. Solution must support a way to avoid device congestion by automatically disabling filters that trigger excessively.

xix. Solution must provide protection against the latest advanced malware threats.

xx. Solution must provide reputation feeds that are updated multiple times a day.

xxi. Solution must provide continuous analysis and re-evaluation of reputations based on activity, source, category, and threat.

xxii. Solution must provide DNS reputation filtering.

xxiii. Minimum SSL inspection for main data center, back-up data center and DR Site required is 3.5Gbps.

xxiv. SSL inspection requirement is for 2K keys with ECDHE-RSA-AES256-GCM-SHA384.

xxv. IPS sizing should be based on the throughput mentioned and shouldn’t be based on number of users or devices in operation.

xxvi. Latency requirement is less than <60 µs.

xxvii. The appliances quoted for main data center, back-up data center and DR Site should be able to inspect minimum 08 segments with copper bypass modules.

xxviii. The appliances quoted for remote sites should be able to inspect minimum 04 segments with copper bypass modules.

xxix. Solution must support asymmetric traffic.

xxx. Solution must support layer 2 fallback.

xxxi. Solution must support hitless reboot.

xxxii. Solution must have high mean time between failure.

xxxiii. Solution must be able to help create custom IPS filters.

xxxiv. Solution must support traffic mirroring from one port to another.

A.2.4 MANAGED SERVICES AND RESPONSE

i. MDR services 1 Gbps Network throughput.

ii. Proposed services must include investigation and response platform that can connect endpoint, servers, and network for correlation.

iii. 24x7x365 (alert investigator), (incident responder), (threat hunter/forensic) analyst and (SOC Manager) at their local/regional/international locations to ensure purchase services are monitored and remotely managed vigorously.

iv. Use machine and human elements to analyze millions of events in real-time.

v. Continuous threat hunting of in-scope assets.

vi. In case of any end point compromise-related threats, the detailed forensic report shall be provided of the incident.

vii. Vendor shall be responsible for providing complete security to the network, its systems against all/any threat, including but not limited to (cyber-attacks, hacking, data lost due to viruses, ransomware attacks, bugs, security breaches, gaining unauthorized access to network and systems.

viii. There must be monthly and quarterly reporting demonstrating the summarized view of catered alerts/offences/incidents detected in each month for the management perspective.

ix. The proposed managed detection response (MDR) service must provide investigation and response proactive outreach including indicator of compromise (IoC) sweeping.

x. Proposed service must provide round-the-clock managed protection against modern evasive threats.

xi. Proposed services must provide visibility across your entire network, analyzing network traffic and hunting for threats.

xii. The proposed MDR service must include impact analysis and response guidance.

xiii. Conducts in-depth investigations of endpoint security alerts and incidents while using proven techniques and expertise to investigate the origin of the compromise, the extent of the breach, and malicious actor attribution and intent.

xiv. Monthly reporting about the incident response and alerts.

A.2.5 SPECIAL CONDITIONS

a. Offeror MUST quote all of the items of an individual Lot.

b. Offeror may opt to quote both the Lots or a single Lot.

c. Lot wise awards will be made.

d. System and solutions supplied under this solicitation will be subjected to testing and inspection by PITC and PSIA.

e. The successful offeror(s) shall provide warranty for successful operation of the system including its maintenance and repair (free of cost) as and when required within three years of the supply and installation.

f. The successful offeror(s) shall extend all possible support and ensure integration and successful operation of the system within the minimum warranty period of three years.

ATTACHMENT B: BILL OF QUANTITIES

B.1 BILL OF QUANTITY TABLE(S)

The cost proposal that will include the Price Quotation Table(s) must be submitted as a separate/standalone document. Pricing must be fully comprehensive, complete, and list any available discounts.

Pricing information supplied with the proposal must be valid for at least 90 days after the due date for proposal submission. All one-time and recurring costs must be fully described. Rates should be quoted, inclusive of all but showing separately, costs of inspection, services, transportation, taxes, import duties if any, and other levies. Payment is to exclude General Sales Tax (GST) and/or import duties for which ESG is exempted as a USAID subcontractor. Pakistani firms will be paid the total amount after deducting withholding tax, which ESG will pay direct to the Federal Board of Revenue (FBR). GST exemption certificate will be provided by ESG upon supplier's request.

Mathematical errors will be corrected in the following manner: If a discrepancy exists between the total price proposed and the total price resulting from multiplying the unit price by the corresponding amounts, then the multiplied unit price will prevail, and the total price will be corrected. If there were a discrepancy between the numbers written out in words and the amounts in numbers, then the amount expressed in words will prevail. If the offeror does not accept the correction, the offer will be rejected.

BILL OF QUANTITY

LOT – 1 Network Devices

Network Devices				Price US $	
	Items and Description		Qty.	Unit Rate	**TOTAL Price***
1	CISCO Router	Cisco ISR 4461 (2x10GE+4x1GE,3NIM,3SM,8G FLASH,4G DRAM)	3		
2	Firewall	Cisco ASA5512-IPS-K9 ASA 5512-X with IPS, SW, 6GE Data	3		
3	CISCO Core Switch	Cisco MDS 9132T 32-Gbps 32-Port Fiber Channel Switch	6		
4	Server	2x Intel® Xeon® Gold 6248R 3.0GHz, 24C/48T or higher 2TB RAM, 1 x 2TB SSD	3		
5	Fiber Channel Card	FC HBA 32 GB Dual Port SFP+ (2xmulti mode optical trans receiver)	12		
6	Fiber Glass Patch Cables	2 Meter Length	15		
		5 Meter Length	10		
		10 Meter Length	5		
				TOTAL US $	

***Please provide separate line item(s) as Taxes**

LOT – 2 Data Center - Cyber Security Solution

Smart Protection Complete Suit for User Protection (Layered Security)	Price US $*
1- ***Supply, installation, testing, and commissioning of End-user Security Module***	
- Threat Protection - Sandbox - Device Control - Endpoint Data Encryption - Mobile Security - Endpoint Detection and Response (EDR) - Email Security - Security for MS Exchange - Data Leakage Prevention Control - Web Gateway Security	For 1,001 Users
2- ***Supply, installation, testing, and commissioning of Data Center (Server Security) Module***	
- Deep Security Enterprise, Virtual Patching - DDoS Protection, Advance Malware Protection	For 125 Servers
3- ***Supply, installation, testing & commissioning of Network Security Module***	
- Network Anti-APT Solution - Next Generation Intrusion Prevention System (IPS)	Single Solution
TOTAL US $	

***Please provide separate line item(s) as Taxes**

B.2 DESTINATION

Equipment/Hardware/Software: All items in this procurement must be delivered to the CEO, Power Information Technology Company (PITC), Room 405 WAPDA House, Shahrah-e-Quaid-e-Azam Lahore, Pakistan as per the delivery schedule. Delivery due date includes the time required for customs clearance for imported items if applicable.

ATTACHMENT C: OFFEROR REPRESENTATIONS AND CERTIFICATIONS

1) Organizational Conflict of Interest* Representations

The Offeror represents, to the best of its knowledge and belief, that this award:

does [ ] or does not [ ] involve a personal or an organizational conflict of interest.

The Offeror represents that it is [ ] is not [ ] owned or controlled in total or in part by any entity of any government.

The Offeror represents that its subcontractors proposed, if any, are [ ] are not [ ] owned or controlled in total or in part by any entity of any government. If no subcontractors are proposed check none [ ] here.

**Please see FAR 9.5 for further explanation.*

2) Source and Nationality of Supplier of Goods, Services, and Commodities

(i) This is to certify that the offeror is:

(a) If an individual, be a citizen or lawful permanent resident (or equivalent immigration status to live and work on a continuing basis) of a country in Code 937

(b) If an organization,

(1) Be incorporated or legally organized under the laws of a country in Code 937;

(2) Must be operating as a going concern in a country in Code 937; and either

(3) Be managed by a governing body, the majority of whom are citizens or lawful permanent residents (or equivalent immigration status to live and work on a continuing basis) of countries in Code 937, or

(4) Employ citizens or lawful permanent residents (or equivalent immigration status to live and work on a continuing basis) of a country in Code 937 in more than half its permanent full-time positions and more than half of its principal management positions.

(ii) This is to certify that the Source (the country from which a commodity is currently located for sale or is to be shipped from) of the Equipment to be supplied under this Order is:

name of country or countries

By signing below, the offeror certifies that the representations and certifications made, and information provided herein, are accurate, current, and complete.

Signature: _____ Date: _____

Name of and title of authorized signature: _____

3) **CERTIFICATION REGARDING LOBBYING**

By signature of its authorized representative below, Subcontractor hereby agrees and certifies, to the best of its knowledge and belief, as follows:

(1) No U.S. Federal appropriated funds have been paid to any person for influencing or attempting to influence an officer or employee of any agency, a member of the U.S. Congress, an officer or employee of Congress, or an employee of a member of Congress, on Subcontractor's s behalf in connection with the awarding of the Prime Contract, or this Subcontract.

(2) If any registrants under the Lobbying Disclosure Act of 1995 have made a lobbying contact on behalf of Subcontractor with respect to the Prime Contract, or this Subcontract, Subcontractor shall complete and submit to ESG OMB Standard Form LLL, Disclosure of Lobbying Activities, to provide the name of the registrants. Subcontractor need not report regularly employed officers or employees of Subcontractor to whom payments of reasonable compensation were made.

(3) The undersigned shall require that the language of this certification be included in the award documents for all subcontracts at all tiers and that all lower-tier subcontractors shall certify and disclose accordingly.

Submission of this certification is a prerequisite for making or entering into this Subcontract imposed by 31 U.S.C. § 1352. Any person who makes an expenditure prohibited under FAR 52.203-12, Limitation on Payments to Influence Certain Federal Transactions, or who fails to file or amend the disclosure required to be filed or amended by this certification, shall be subject to a civil penalty of not less than $10,000, and not more than $100,000, for each such failure.

Signature: _____

Typed Name: _____

Title: _____

Date: _____

4) FAR 52.222-56 CERTIFICATION REGARDING TRAFFICKING IN PERSONS COMPLIANCE PLAN.

By signature of its authorized representative below, Subcontractor hereby certifies to ESG and USAID that –

(1) Subcontractor has implemented a compliance plan to prevent any prohibited activities identified in paragraph (b) of FAR 52.222-50, Combating Trafficking in Persons (OCT 2020) and to monitor, detect, and terminate any agent, lower-tier subcontract, or lower-tier subcontractor employee engaging in prohibited activities; and

(2) After having conducted due diligence, either –

(a) To the best of Subcontractor's knowledge and belief, neither it nor any of its agents, lower-tier subcontractors, or their agents is engaged in any such activities; or

(b) If abuses relating to any of the prohibited activities identified in paragraph (b) of the aforementioned FAR clause have been found, Subcontractor or lower-tier subcontractor has taken the appropriate remedial and referral actions.

Signature: _____

Typed Name: _____

Title: _____

Date: _____

5) FAR 52.204-23 PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES.

PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES (NOV 2021)

(a) *Definitions*. As used in this clause—

Covered article means any hardware, software, or service that–

(1) Is developed or provided by a covered entity;

(2) Includes any hardware, software, or service developed or provided in whole or in part by a covered entity; or

(3) Contains components using any hardware or software developed in whole or in part by a covered entity.

Covered entity means–

(1) Kaspersky Lab;

(2) Any successor entity to Kaspersky Lab;

(3) Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or

(4) Any entity of which Kaspersky Lab has a majority ownership.

(b) *Prohibition*. Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91) prohibits Government use of any covered article. The Contractor is prohibited from—

(1) Providing any covered article that the Government will use on or after October 1, 2018; and

(2) Using any covered article on or after October 1, 2018, in the development of data or deliverables first produced in the performance of the contract.

(c) *Reporting requirement*.

(1) In the event the Contractor identifies a covered article provided to the Government during contract performance, or the Contractor is notified of such by a subcontractor at any tier or any other source, the Contractor shall report, in writing, to the Contracting Officer or, in the case of the Department of Defense, to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) The Contractor shall report the following information pursuant to paragraph (c)(1 of this clause:

(i) Within 1 business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; brand; model number (Original Equipment Manufacturer (OEM) number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the report pursuant to paragraph (c)(1) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of a covered article, any reasons that led to the use or submission of the covered article, and any additional efforts that will be incorporated to prevent future use or submission of covered articles.

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

(End of clause)

The Offeror Certifies that no Prohibited items (as described in the above clause) are being offered or will be provided in response to this RFP.

Offeror: _____

Date: _____

6) FAR 52.204-24 REPRESENTATION REGARDING CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT

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)

7) FAR 52.204-26 COVERED TELECOMMUNICATIONS EQUIPMENT OR SERVICES-REPRESENTATION

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)