Mock Task Order Request for Proposal #2:
Penetration Testing
Professional Services RFP – IT Security Services

CAPITALIZED TERMS USED BUT NOT DEFINED IN THIS TORP HAVE THE MEANING SET FORTH IN PROFESSIONAL SERVICES CONTRACT # USAC-20-015 (THE "CONTRACT"). AND THIS TORP IS ISSUED PURSUANT TO AND UNDER THE TERMS AND CONDITIONS SET FORTH IN THE CONTRACT.

I. TASK ORDER TYPE

USAC intends to award a single, firm-fixed price, task order for Penetration Testing under the IT SECURITY SERVICES service category, under the Contract. The firm fixed price is to include all direct and indirect costs set forth in this Section B, including equipment, product support, supplies, general and administrative expenses, overhead, materials, travel, labor, taxes (including use and sales taxes), shipping, and profit. USAC will not reimburse Contractor for any travel-related expenses.

II. BACKGROUND

Through its administration of the USF programs on behalf of the FCC, USAC works to promote the availability of quality services at just, reasonable and affordable rates and to increase access to advanced telecommunications services throughout the nation. Specifically, the USF programs provide funding for the expansion of telecommunications and broadband access to rural communities and health care facilities, schools and libraries across the country, and low income households. Through program administration, auditing, and outreach, USAC works with contributors, service providers, and program beneficiaries to achieve the program goals articulated by the FCC for each of these programs.

III. PURPOSE OF THE TORP

The purpose of the USAC Financial Operations System is to serve as the general ledger for the Fund and the source for all financial records, which are kept in Microsoft Dynamics Great Plains (GP). Records for the Fund are tracked in detail through Microsoft Dynamics GP in the USFGL company installation, and all operational expenditures related to the functioning of the Universal Service Administrative Company are stored in the USAC company installation. These are validated by the financial operations and accounting team. This includes all account balances, receivable details, payable details, and disbursement details. The Microsoft Dynamics GP system is one of the major applications involved in financial controls. Billing, collections and disbursements records are loaded into Microsoft Dynamics GP at periodic times during the month. Budgets are formulated based on actual transactions from Microsoft Dynamics GP in Power Plan and after those budgets are approved are entered back into Microsoft Dynamics GP.

Account balances are aged and kept in Microsoft Dynamics GP for contributors. There are only internal users, which include the Finance and IT support staff of USAC. There are no external users.

Financial Operations System consists of the following major software components:

1. **Microsoft Dynamics GP 2015**: Contains summary and detailed financial transactions and produces financial statements. Major customizations to the USFGL Company of Microsoft Dynamics GP include: Mass Apply, to apply payments and credits to receivable balances in a manner that is not supported by the system itself; and Disbursements Automation, to automate integration of authorized disbursement information, offsetting between AP and AR balances and remittance statement generation. Contributor, service provider and SL applicant records are updated in real time by data from E-File and EPC. SL applicant receivables are loaded nightly from EPC. Universal Service Fund disbursement information is loaded from High Cost (HC), Lifeline (LI), Rural Healthcare (RH), SL and SA systems periodically during the month. Vendor payments related to USAC administration are processed through the JP Morgan web site.
2. **Billing**: Calculates and generates monthly Universal Service Fund contributor invoices. Maintains historical contributor invoice information. Receives contributor information from E-File and contributor balance information from the USFGL Company of Microsoft Dynamics GP, and sends new invoice information back to the USFGL Company of Microsoft Dynamics GP.
3. **Redlight**: Identifies companies that should not receive Universal Service Fund disbursements from USAC and/or should have their disbursements reduced by the amount they owe USAC. Receives contributor company information from E-File and contributor debt information from the USFGL Company of Microsoft Dynamics GP and the FCC. Sends Redlight hold information to the USFGL Company of Microsoft Dynamics GP.

USAC is committed to ensuring the security and protection of the data that is collected, used, and stored in its IT systems that support the four universal service programs described above. To ensure the security and protection of its IT systems and data, USAC is seeking a best-in-class provider who will conduct Penetration Testing on its IT systems to assess the systems and detect security flaws and issues consistent with the NIST Special Publications (SP) 800-115, 800-53, rev. 4, and 800-37, rev. 2 and FISMA requirements.

IV. TASK ORDER PERIOD OF PERFORMANCE

The period of performance for the Task Order is four weeks (the "Term"). The Task Order shall expire at the end of the Term unless extended, in writing, by USAC.

V. PLACE OF PERFORMANCE

Contractors shall perform Task Orders at either its own facilities or at USAC Headquarters. Occasional meetings may be conducted at USAC's Headquarters or at the FCC offices located at 445 12th Street SW, Washington, DC 20554. USAC shall provide appropriate office space and appropriate access to its computer network for duties performed at USAC Headquarters, if necessary. Contractors will be required to complete USAC's Visitor Form, USAC Visitor Form and wear a badge while on USAC premises.

VI. TASK ORDER PROCESS

Attachment 1 Pricing. Fixed labor-hour rates for T&M must be fully burdened and include all wages, overhead, general and administrative expenses, taxes and profit, and individual laptop equipment and office software for each category of labor. Services for the T&M CLINS shall be performed on a T&M basis using the labor categories and fixed hourly rates set forth in Attachment

A. ***Task Order Ceiling Price.*** Each Task Order issued under the Contract will include a ceiling price (the "Task Order Ceiling Price"). USAC will not be obligated to pay Contractor any amount in excess of the Task Order Ceiling Price, and Contractor shall not be obligated to continue performance if to do so would exceed the Task Order Ceiling Price, unless and until USAC notifies Contractor in writing that the Task Order Ceiling Price has been increased and specifies in the notice a revised ceiling price that shall apply to the Task Order.

B. ***Steps for each Task Order***

1. Issuance of Task Orders. USAC will issue Task Orders in accordance with the procedures set forth below. As specified in each Task Order issued under the Contract, Contractor shall provide experienced personnel who are capable of performing the tasks described in, and who meet the qualifications listed under, the Key Personnel set forth below.

2. Work Schedule. Unless otherwise specified in a Task Order, Contractor personnel assigned to a Task Order shall maintain a work schedule consistent with USAC normal business hours and work practices. Contractor personnel are expected to comply with all of USAC's rules pertaining to conduct in the workplace. Any change in Contractor personnel must be approved, in writing, by the USAC Procurement department and reflected in the Task Order. Contractor personnel are not employees of USAC.

3. Invoicing and Reporting Instructions. Each Task Order will outline the invoicing and reporting instructions required specifically for that project.

4. Task Order Proposals. Contractor shall perform the following steps which are necessary for the Task Order award. Contractor shall submit one proposal in response to each TORP. See Attachment 1, Mock TORP. Each Contractor proposal in response to a TORP must include the following information:

a. *Basic Information*. A cover page which includes:
   1. The name of Contractor's organization;
   2. Offeror's contact name;
   3. Offeror's contact information (address, telephone number, email address, website address);
   4. Offeror's DUNS number;
   5. The date of submission;
   6. A statement verifying the proposal is valid for a period of 120 days; and
   7. The signature of a duly authorized Offeror representative.

b. *Production Schedule*. A detailed and comprehensive production schedule that includes a proposed schedule and approach for managing and providing the Services and Deliverables required by the TORP. Contractor should also outline any deviations from the TORP.

c. *Pricing*. A total hourly breakdown of each Contractor proposed staff.

d. *Ceiling Price*. A proposed Task Order ceiling price for the TORP, as well as a justification.

C. ***Task Order Proposal Review***. USAC will review Contractor's proposal to this TORP, provide feedback if any adjustments or negotiations are required, and subsequently award the Task Order.

VII. SCOPE OF SERVICES AND DELIVERABLES

Each of the below systems require the Contractor to test as follows:

A. Financial Operational System (FOS)

1. Items In Scope:

a. Internal Network Vulnerability Assessment and Penetration Testing
b. Access Control Testing - verify whether entry points to the USAC internal infrastructure are properly secured.
   i. VPN Configuration Review
   ii. Citrix Configuration Testing and Review
   iii. Password Cracking
c. Server Configuration Review
d. Software Source Code Review - static application security testing (SAST) to analyze source code and/or compiled versions of code to discover security vulnerabilities.
e. Application Threat Modeling and Design Review - identify, quantify, and address the security risks associated with an application; supplements Software Source Code Reviews.

2. **Items Out of Scope:**
   a. Network Penetrating Testing – evaluation of the network perimeter and firewall from the perspective of an outside attacker with no inside knowledge of the network.
   b. External Web Application Testing – testing of public facing web application to discover web design vulnerabilities with respect to the top 10 most common exploits (OWASP Top 10).
   c. Attempting any designed Denial of Service vulnerabilities or exploiting vulnerabilities (actual enumeration and penetration).

A. DELIVERABLES

USAC will oversee the security penetration tests in 2020, as each system undergoes Risk Management Framework (RMF) Step 4 enhanced security testing.

A. **Types of Penetration Testing.** The boundary and parameters for each penetration test will be determined by system, each system will contain one (1) or more of the following Penetration Tests Service Categories.

1. *Penetration and Vulnerability Testing*
   a. Application and Network Penetration Testing Services

   The contractor shall provide Application and Network Penetration Testing Services including based on the first two steps of penetration testing process consisting of foot printing and scanning.

   The general testing services will include, but not limited to:

   - Network Foot printing (Reconnaissance)
   - Discovery, Scanning, Probing
   - Internal Network Vulnerability Assessment and Penetration Testing
   - Access Control Configuration Testing
   - Server Specific Configuration Testing
   - Network Backbone Testing

B. **Rules of Engagement.** All parties must agree to the Rules of Engagement ("ROE"), for each system, in writing, before the commencement of each penetration testing scenario. The ROE documents will include, but may not be limited to:
   1. Scope;
   2. Timeline;
   3. Methodology / Approach;
   4. Tools;
   5. Notification procedures;
   6. Information that must be provided to pen test team (e.g. IP ranges, application URL, etc.);
   7. Reporting; and

8. Points of contact.

C. **Timeline for testing each system.**

1. Penetration testing activities, for each system, must not exceed four (4) weeks. *See* Section B.III for number of systems testing during each phase. Up to five (5) systems may run concurrently, with the same deadlines.

2. The following represents USAC's anticipated Contract activity, broken up by week:
   a. Week 1 - Preparation/Data Gathering/Discovery/Kickoff meeting
   b. Week 2 – Penetration Test/ Remediation Work
   c. Week 3 – Remediation Work/Retest/Draft Penetration Test Report
   d. Week 4 – Write/Deliver Final Penetration Test Report

3. During each information system's testing period (weeks 1 through 4), there must be a feedback loop built in between the pen testers and the System Owner such that there is a recursive built-in process for addressing critical and high findings discovered during testing activities, and suggesting remediation activities. In order to meet hard deadlines, multiple system Penetration Testing will need to run concurrently.

D. **Deliverables.** At the end of each phase of the four (4)-week projects, the Contractor will deliver the required NIST 800-53, rev. 4 and NIST 800-115 Penetration Testing deliverables detailed in this section. The primary deliverable for each USAC system being tested will be a report detailing all findings discovered during the assessment. This report will include:

1. An *Executive Summary* report that summarizes the scope, approach, findings, and recommendations in a manner suitable for senior management.

2. A summary table outlining the findings, their risks, and the number of instances of each finding.

3. A written documentation for each location of the approach, findings, and recommendations associated with this project/task order:

   a. A formal presentation of the findings and recommendations to senior management may also be required.

   b. A detailed *Technical Report* for the use of each organization's technical staff which discusses: the methodology employed, positive security aspects identified, detailed vulnerability findings, and assignment of a risk rating for each vulnerability, supporting detailed exhibits for vulnerabilities when appropriate, and detailed technical mediation steps. A description of the vulnerability explaining the vulnerability and a few possible ways an attacker may be able to exploit it.

   c. A list of every instance of the vulnerability discovered during the assessment. This will include the affected uniform resource locator (URL) and parameter if applicable.

d. Steps to reproduce the issue for a minimum of two (2) instances of the vulnerability.

e. Evidence that the vulnerability exists for a minimum of two (2) instances of the vulnerability. Evidence may include a screenshot, HTTP Request/Response, source code, or similar evidence.

Deliverable	Due Date
Penetration Testing Complete	End of week 2
Final Penetration Report	End of week 4

VIII. KEY PERSONNEL & LABOR CATEGORIES

A list, by name, of all Key Personnel, along with the labor category they will fill. For each Key Personnel, Contractor shall provide a biography that includes his/her educational background, skill-set, job and related experience, a list of specific efforts he/she has supported, and references. Contractor shall provide a Relationship Manager ("RM") who shall ensure the completion and delivery of the Task Order and serve as a single point of contact for the day-to-day management of the Task Order.

All pricing information for the TORP shall be based on Contractor's Attachment 1: Bid Sheet to the Contract.

IX. INVOICES

Where to Submit Invoices. Contractor shall submit invoices through the USAC Coupa Supplier Portal ("CSP") method or via the Supplier Actionable Notification ("SAN") method. The CSP method will require Contractor to register and create an account for the CSP. An invitation link to the CSP may be obtained by emailing CoupaHelp@usac.org. The SAN method will require Contractor to invoice USAC directly from the purchase order ("PO") sent by USAC via email. For the SAN method, the USAC email will contain a notification with action buttons which will allow Contractor to create an invoice, add a comment, and acknowledge the receipt of the PO. For assistance on all Coupa related billing questions, Contractor may email CoupaHelp@usac.org. For assistance on all non-Coupa related billing questions, Contractor may email accounting@usac.org.

Invoice Submittal Date. Contractor may submit invoices for payment upon completion and USAC's acceptance of all of the work associated with a Contract or, if the period of performance of a Contract exceeds sixty (60) days, once every thirty (30) days, with the submission of the first invoice no earlier than thirty (30) days after issuance of the Contract.

Content of Periodic Invoices. If periodic invoices are submitted for a Contract, each invoice shall include only Services that have been completed and Deliverables that have been accepted as of the date of invoice submission and that have not been billed in a prior invoice.

X. COMMUNICATION

Contractor shall be reasonably available and accessible via email or telephone during USAC's normal business hours, which are Monday through Friday (9:00AM-6:00PM ET). When necessary, communication may be made outside of these hours to ensure the progress of the Contract is not impeded.

XI. MEETINGS

During performance of the Task Order, Contractor personnel shall communicate on a regular basis with USAC staff, and, as requested by USAC's COR or CA, attend status meetings with USAC staff to discuss project status and progress, impediments, and audit findings. Status meetings will be held by either teleconference or in person. Status reports may be used as the basis of the status meeting discussions.

XII. TRAVEL

Contractor staff may be required to travel to USAC to perform Services under the Task Order. Contractors may invoice for up to 10% of the total Task Order value in travel expenses, provided Contractor complies with the terms and conditions of the USAC travel policies. All Contractor travel costs should be included in the Contractor's proposed Task Order Ceiling Price.

XIII. TASK ORDER PROPOSAL SUBMISSION INSTRUCTIONS

All responses, to this TORP, are due no later than **11:00 AM ET, March 12, 2020**. Responses received after this date and time or do not follow the task order submission instructions, may not be considered for review.

Responses should be prepared simply and economically, and provide a straightforward and concise explanation of the information requested. Emphasis should be on completeness and clarity.

Please submit one (1) electronic copy (PDF) of your response to Becca Wray at rfp@usac.org. All submissions must include "Response to Mock Task Order #02 – Penetration Testing - FOS" in the subject line. Please note: all electronic submissions must be limited to a maximum size of 25 GB.