Universal Service Administrative Co.

USAC Request for Information (RFI)
IT-25-188 - Penetration Testing as a Service

REQUEST INFORMATION:

Method of Solicitation:	Request for Information ("RFI")
RFI Number:	RFI IT-25-188
RFI Issue Date:	November 17, 2025
Question Due to USAC:	November 24, 2025, by 11:00 AM ET
Q&A Response Release Date:	November 28, 2025, by 5:00 PM ET
RFI Due Date:	December 8, 2025

RFI ISSUED BY:

Universal Service Administrative Co.
700 12th Street, NW, Suite 900
Washington, DC 20005

CONTACT INFORMATION

USAC CONTACT INFORMATION	OFFEROR CONTACT INFORMATION
Mustafa Kamal Procurement Specialist P: 202-423-2615 E: Procurement@usac.org Mustafa.Kamal@usac.org	(complete) Name: _____ POC: _____ POC Title: _____ POC Phone: _____ POC Email: _____ Address: _____

Universal Service Administrative Co.

1. ABOUT US

Through its administration of the Universal Service Fund ("USF") programs on behalf of the Federal Communications Commission ("FCC"), USAC works to promote the availability of quality telecommunications 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, 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 the High Cost Program, Lifeline Program, Rural Health Care Program, and Schools and Libraries Program.

USAC strives to provide efficient, responsible stewardship of the programs, each of which is a key national asset in making important telecommunications and Internet services available to consumers, health care providers, schools, and libraries throughout the United States. The program divisions are supported by additional USAC personnel in other divisions, including Finance, Office of General Counsel ("OGC"), Information Systems, Audit and Assurance, Enterprise Process Improvement ("EPI"), and Human Resources ("HR").

Consistent with FCC rules, USAC does not make policy nor interpret unclear provisions of statutes or the FCC's rules. The USF is funded by contributions from telecommunications carriers, including wireline and wireless companies, and contributions from interconnected voice over internet protocol ("VoIP") providers, including cable companies that provide voice service, based on an assessment of their interstate and international end-user revenues. These contributions are typically passed through to consumers through a universal service fee line item on their telephone bills.

HIGH COST PROGRAM

The High Cost Program is designed to ensure that consumers in rural, insular, and high-cost areas have access to modern communications networks capable of providing voice and broadband service, both fixed and mobile, at rates that are reasonably comparable to those in urban areas ("High Cost"). High Cost fulfills this universal service goal by allowing eligible carriers who serve these areas to recover some of their costs from the USF. Like all USF programs, the administration of High Cost has undergone significant modernization in the last several years to increase innovation and ensure beneficiaries have access to updated technology. USAC developed and now leverages the High Cost Universal Broadband Portal ("HUBB"), which allows participating carriers to file deployment data showing where they are building out mass-market, high-speed internet service by precise location. This information includes latitude and longitude coordinates for every location where service is available, and USAC displays this information on a public-facing map to show the impact of high-cost funding on broadband expansion throughout the United States.

LIFELINE PROGRAM

Universal Service Administrative Co.

The Lifeline Program provides support for discounts on broadband and voice services to eligible low-income households ("Lifeline"). USAC uses its centralized application system, the Lifeline National Eligibility Verifier ("National Verifier"), to verify consumer eligibility through proof of income or the consumer's participation in a qualifying federal benefit program, such as Medicaid, the Supplemental Nutritional Assistance Program ("SNAP"), Federal Public Housing Assistance, or Veterans and Survivors Pension Benefit. USAC focuses on metrics and data analytics for Lifeline improvement and provides outreach efforts to eligible households to increase participation in and the effectiveness of Lifeline. USAC also works to ensure program integrity by supporting the needs of Lifeline stakeholders, reducing program inefficiencies, and combating waste, fraud, and abuse. USAC reviews processes regularly to increase compliance, identify avenues for operational improvements, and refine program controls, such as audit processes.

RURAL HEALTH CARE PROGRAM

The Rural Health Care Program supports health care facilities in bringing medical care to rural areas through increased connectivity ("RHC"). RHC consists of two main component programs: (1) the Telecommunications Program ("Telecom") and (2) the Healthcare Connect Fund Program ("HCF"). The FCC established Telecom in 1997 to subsidize the difference between urban and rural rates for telecommunications services. Under Telecom, eligible rural health care providers can obtain rates on telecommunications services in rural areas that are reasonably comparable to rates charged for similar services in corresponding urban areas. In 2012, the FCC established HCF to promote the use of broadband services and facilitate the formation of health care provider consortia that include both rural and urban health care providers. HCF provides a discount on an array of advanced telecommunications and information services such as Internet access, dark fiber, business data, traditional DSL, and private carriage services. These telecommunications and broadband services support telemedicine by ensuring that health care providers can deliver cutting edge solutions and treatments to Americans residing in rural areas.

SCHOOLS AND LIBRARIES PROGRAM (E-RATE)

The Schools and Libraries Program helps schools and libraries obtain high-speed Internet access and telecommunications services and equipment at affordable rates ("E-Rate"). E-Rate provides a discount for the cost of broadband and telecommunications services to and within schools and libraries in order to support a modern and dynamic learning environment. Applicants and service providers submit FCC Forms (e.g. requests for services or funding) and other compliance-related documentation to the E-Rate Productivity Center ("EPC"), an electronic platform that enables participation in the program. USAC frequently invests in new tools and data analytics capabilities to support the success of the program in alignment with the FCC's goals.

Additional information on USF programs can be found at: USAC | About | Universal Service.

Universal Service Administrative Co.

2. COMPANY PROFILE

USAC is a not-for-profit Delaware corporation operating under the oversight of the FCC. USAC is not a federal agency, a government corporation, a government controlled corporation or other establishment in the Executive Branch of the United States Government. USAC is not a contractor to the federal government. Any Contract to be awarded as a result of a subsequent RFP from this RFI will not be a subcontract under a federal prime contract. USAC does, however, conduct its procurements in accordance with the terms of a Memorandum of Understanding with the FCC, which requires USAC to adhere to the following provisions from the Code of Federal Regulations: 2 C.F.R. §§ 200.318-321; 200.324; 200.326-327 and App. II to C.F.R. Part 200 (collectively "Procurement Regulations"). Further, USAC IT Systems that are used to administer the USF programs and USAC vendors that handle and manage USF data must be compliant with FISMA and NIST requirements as applicable to federal agencies.

3. PURPOSE

The Universal Service Administrative Company ("USAC") is issuing this Request for Information (RFI) seeking information from US-based companies with the ability to provide Penetration Testing as a Service (PTaaS). The goal of this RFI is to provide USAC with the latest information on cloud based software services that are available to execute a variety of services to remotely test USAC Information Technology (IT) systems for vulnerability to penetration attacks. ***Please note that this is not a solicitation for products and/or services and this inquiry will not result in an award or contract.***

The specifications and information gathered from responses to this RFI will be used to evaluate the offerings of the current marketplace and may lead to the development and preparation of a formal Request for Proposal (RFP). For simplicity USAC will refer to Penetration Testing as a Service as 'PTaaS' throughout the remainder of this RFI.

USAC is soliciting information from Cloud Service Providers ('CSP') and other interested parties capable of assisting USAC in identifying a PTaaS provider that either can remotely execute penetration testing, to include both technical and social engineering related methods, for USAC's mission systems. Furthermore, USAC would also be interested in the provider also providing support with the configuration, customization, implementation, and training required to work with a remote PTaaS provider to support penetration testing. Information submitted by any interested party will be done so voluntarily and with the understanding that this RFI is for information gathering purposes only and is not a formal solicitation. Similarly, cost ranges will be used solely for budgetary analysis and establishing a target budget. Information presented during this information gathering process will not be considered as a response to any solicitation subsequently issued by USAC.

Respondents may be asked to provide a demonstration of their products and services. This would include a guided tour of their product, business capabilities and technology. Demonstrations may be presented through Internet web conferencing. No compensation will be made by USAC for demonstrations.

Universal Service Administrative Co.

4. TECHNICAL REQUIREMENTS

The following describes a high-level requirements or scope of work for a potential PTaaS engagement subject to a future RFP. USAC is exploring to find out about potential offerors who can provide these required services. In addition, offerors are encouraged to explain what additional services their proposed solutions will offer.

A. Description of Penetration Testing as a Service Requirements:

USAC is soliciting information on available remote penetration testing as a cloud-based service. The main purpose of the tool would be to execute directed penetration tests of USAC systems, networks, and personnel for social engineering awareness and protection. This service would replace annual local and manual penetration tests with dynamic penetration testing available as needed with minimal scheduling parameters for both compliance tests and focused tests for emerging threats. The service should also include social engineering tests to assess USAC personnel vulnerabilities for fraudulent attempts to infiltrate USAC through people with access, authority, or influence at USAC.

USAC expects that the service can be requested for any system to test in a production-like test environment to identify systemic failures, vulnerabilities, or misconfigurations that represent opportunities for malicious attacks.

USAC is interested in the variety of methods a PTaaS provider would use for testing applications, networks, and systems such as black/grey/white box testing, threat emulation, layered testing, network attacks, and data poisoning or related AI attacks. The PTaaS provider should simulate tactics, techniques, and procedures (TTPs) used by real-world adversaries. The PTaaS provider should offer and remain aligned with best practice such as NIST SP 800-115, the OWASP Testing Guide, and the Penetration Testing Execution Standard (PTES).

USAC is interested in the potential for nominally invasive penetration testing for production applications, web applications, and reactionary testing based on imminent threats, known exploited vulnerabilities (KEV), or identified vulnerabilities.

Social engineering is a form of penetration testing that USAC sees as a growing threat, particularly with AI enhanced emulation of actual communications and web presence. USAC expects the service to provide enhanced testing of social engineering resistance and continuous update of this kind of penetration test as capabilities and methods grow more sophisticated with the use of AI.

For all penetration testing, USAC expects the PTaaS provider to provide close coordination with USAC IT Security for planning, execution, reporting, and continuous feedback to include escalation for impactful findings that need remediation. USAC also expects support to retest remediated findings from the PTaaS provider.

USAC is interested in the possibilities of the PTaaS providing physical access testing and wireless network testing at USAC's DC Headquarters.

Universal Service Administrative Co.

B. Expected Technical Scope of Work:

USAC expects the technical scope of the PTaaS testing would include:

- External Network Testing:
  - Public-facing IP addresses, firewalls, VPNs, and web applications, without conflicting with USAC's Vulnerability Disclosure Program

- Internal Network Testing:
  - Internal servers, workstations, domain controllers, network segmentation
  - Wi-Fi access points, encryption protocols, rogue device detection
  - Remote access infrastructure and services
  - Identity and access management
  - From 800 to 1200 USAC-issued/managed laptops

- Application Testing
  - OWASP Top 10 vulnerabilities, authentication mechanisms, input validation
  - Mobile applications used to access USAC resources
  - Web applications, both internal and mission systems

- Social Engineering
  - Such as phishing simulations, pretext calling, physical access attempts

- Cloud Service Provider Testing
  - Infrastructure as a Service (IaaS) for system and general services
  - Platform as a Service (PaaS) for certain USAC systems
  - Software as a Service (SaaS) when integrated with USAC systems and general services

C. Potential Assumptions:

USAC asks for consideration of the following assumptions:

- USAC will provide necessary access, credentials, and documentation
- Testing will be conducted during agreed-upon hours to minimize disruption
- All findings will be treated as confidential and shared only with authorized personnel

D. Overview of Potential Engagement:

USAC expects a potential PTaaS acquired engagement subject to a potential future RFP to include:

- Kickoff meeting, onboarding and finalized rules of engagement
- Overall plan for penetration testing per year
- Training and documentation on using the PTaaS provider's online website and communications

Universal Service Administrative Co.

- Status, progress, and intermediate reports during testing, especially for critical vulnerabilities
- Reports per formal test including
    - Executive summary
    - Detailed findings with CVSS scores
    - Screenshots and proof-of-concepts
    - Risk ratings and business impact
    - Remediation recommendations and stakeholder debriefings
- Re-testing of remediated findings
- Continuous availability of status and progress available via online dashboard

E. High level view of USAC assets for the purpose of estimating cost parameters for proposed services:

- Approximately 18 FISMA authorized system boundaries
- Systems include Windows and Linux operating systems, infrastructure on premises, AWS cloud, hybrid premises-AWS, Microsoft Azure services such as M365, Oracle cloud, and PaaS provider Appian Cloud.
- Internal users include both employees and contractors as well as business process outsourcing (BPO) vendors to augment operations for USAC systems; user count ranges from 1000 to 1500.
- External users of USAC systems are approximately 200,000.
- USAC does not develop mobile applications.
- USAC has about 220 applications/databases with access control.

Note: Responses are encouraged to identify additional functionalities and capabilities that enhance, support, or replace the requirements included in this narrative.

5. PROPOSED RFI TIMELINE

Event	Date
RFI Released	Monday, November 17, 2025
RFI Issue Date	November 17, 2025
Questions Due to USAC	Monday, November 24, 2025, by 11:00 AM ET, Procurement@usac.org
Q&A Response Released	Friday, November 28, 2025, by 5:00 PM ET, Procurement@usac.org
RFI Responses Due	Monday, December 8, 2025, by 11:00 AM ET
Demos (if needed)	TBD, 2025

6. RFI SUBMISSION INSTRUCTIONS

All responses to this RFI are due no later than **Monday, December 8, 2025, by 11:00 AM ET**. Responses received after this date and time may not be considered for review.

Universal Service Administrative Co.

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 USAC at Procurement@usac.org with copy to Mustafa.Kamal@usac.org. In the subject line, all submissions must include "Response to RFI XXX-24-188 – Penetration Testing as a Service".

NOTE: All electronic submissions must be limited to a maximum size of 25 MB.

7. RFI RESPONSE FORMAT

The response must include the following sections and must have numbered pages and include an index or table of contents referencing the appropriate page numbers.

SECTION 1 – ORGANIZATIONAL OVERVIEW

Maximum: Three (3) Pages

Please provide a response that includes the following:

- Years of experience in providing PTaaS solutions.
- Your company's core competencies.
- What differentiates your organization and existing solutions in the market.
- Number of clients you serve with similar solutions.
- How the service will maintain currency and readiness to test for emerging threats

SECTION 2 – PROPOSED TECHNICAL SOLUTION

Maximum: Eight (8) Pages

Please provide a solution response to the associated Penetration Testing as a Service requirements stated in RFI Section 3.Solution descriptions must be concise and directly address the requirements. Your proposed solution must include responses to the following questions:

- Does your organization offer all the services identified in this RFI?
- What additional services are offered that are not identified in this RFI?
- Are any services offered that replace services identified in this RFI?
- Are any services offered that would monitor production systems?
- How do offered services help with identifying AI risk?
- What is the lifecycle of a penetration testing engagement for a system?
- How are offered services priced, i.e., by system size, number of systems, endpoints, etc.?
- How are findings aligned with NIST, FISMA, and other Federal standards?
- What is the FedRAMP status, if at all, for the services offered?

- How do the services address Fraud Risk?

SECTION 3 – EXPERIENCE

Maximum: Two (2) Pages

Responses shall address the following question:

- What relevant corporate experience does the company have with providing PTaaS solutions?
- What is the scope and type of clients for offered PTaaS solutions?
- What is proposed value of PTaaS services compared to on-premises or manual penetration testing services?
- What are experiences with testing applications operating on AWS?
- What are experiences with testing applications operating on Appian Cloud?
- What are experiences with testing solutions using Microsoft 365 and Azure services?
- How will the company keep up with emerging threats and keep the testing competitive?

SECTION 4 – PRICING ESTIMATE

Maximum: One (1) Page

(Note: Any prices provided as part of this RFI are intended solely for budgetary analysis and to establish a reasonable target budget).

Responses shall include a cost estimate for the following:

- Include an estimate for all relevant service components, to include such as service purchases, required software, licenses and ongoing service support.
- Identify how the service is priced, such as by test, ongoing, number of applications, number of users, and all other considerations to support USAC budgeting for such a purchase.

8. OFFEROR INQUIRIES AND QUESTIONS

Questions and inquiries regarding this RFI must be submitted in writing by **Monday, November 24, 2025, by 11:00 AM ET**. Please submit all questions to USAC at procurement@usac.org with copy to Mustafa.Kamal@usac.org. The subject line "Questions to RFI IT-25-188 – Penetration Testing as Service"