Universal Service Administrative Co.

Universal Service Administrative Co. (USAC)
RFP IT-26-027 – Penetration Testing as a Services
Questions & Answers

Q#	Question	Answer
1.	Is there an existing vulnerability management platform in place (e.g., Tenable, Qualys)? If so, will access be provided?	Rapid7, information will be available
2.	Are there any proprietary web applications that require in-depth testing? If so, how many?	About 100
3.	HoSw will internal access be provided if testing is conducted remotely? (e.g., VPN, virtual machine, SSH)	VPN, VMs
4.	Will each system include testing from an Internal and External (if applicable) perspective?	As applicable
5.	Approximately, how many IPs will be included in the scope for each system?	100K IP addresses spread across 201 subnets
6.	Does each system have its own Active Directory/IdM domain or are domains managed at an organizational level?	Organizational level
7.	Are they systems primarily Windows, Linux, or a mix of both?	Primarily Windows, some Linux
8.	Will domain credentials be provided for auditing Active Directory or other domain level configurations?	As applicable
9.	Will access to the cloud environment be provided for configuration review?	As applicable
10.	How many S networks (SSIDs) are in scope?	One (1)
11.	How many physical sites, floors, or buildings are in scope for wireless testing?	2 floors in one building in DC

Universal Service Administrative Co.

Q#	Question	Answer
12.	What wireless technologies are deployed (e.g., 802.11a/b/g/n/ac/ax, WPA2-Enterprise, WPA3, Open networks)?	Corporate wireless is 802.11ac/ax, and authentication is Peap-MSCHAPv2 via 802.1x with device certificates. We have 2 WpA 2 SSIDs that only use a password for iPad devices at the front desk and certain video devices for the service desk.
13.	Are there any legacy authentication mechanisms or deprecated protocols still in use (e.g., WEP, WPA, LEAP, TKIP)?	No.
14.	Will test credentials or certificates be provided for Enterprise Wi-Fi networks?	As applicable
15.	Will rogue access point and de-authentication attacks be permitted?	To be discussed on engagement
16.	Will a list of target personnel be provided?	Yes
17.	Will targets/context require prior approval?	Yes
18.	How many employees will be targeted during phone/email-based social engineering?	Prior phishing campaigns have been enterprise-wide. USAC is open to advice and best experience of vendors.
19.	Are there specific departments (e.g., IT, HR, finance) we should focus on?	To be discussed on engagement
20.	Will the targets be aware of the test (i.e., authorized deception)?	No
21.	Are there specific pretexts you want or don't want us to use?	To be discussed on engagement
22.	Can we spoof internal phone numbers or email domains?	To be discussed on engagement
23.	How many physical locations require access testing?	See #12
24.	For each location, what is the approximate size (e.g., square footage, number of floors)?	See #12
25.	What physical access control systems are in use (e.g., HID, Lenel, Honeywell, custom systems)?	Kastle Systems
26.	What credential types are used (e.g., proximity cards, smart cards, NFC, mobile credentials, biometrics)?	Proximity cards with RFID and Smart Phones

Universal Service Administrative Co.

Q#	Question	Answer
27.	Are temporary badges, visitor badges, or contractor credentials used?	Contractors are issued badges, have special check-in/out requirements, no visitor badges or temp badges are issued
28.	Will access badges be provided for testing, or is badge cloning/bypass expected?	To be discussed on engagement
29.	Are security guards employed on-site or via a third-party vendor? If so, will guards be informed of the assessment in advance, partially informed, or unaware?	Security guards and scanners at entry to building. Engagement with the building security: as needed and to be discussed on engagement
30.	What model types are used (LLMs, classification models, recommendation models, etc.)?	To be discussed on engagement
31.	Are models hosted locally or accessed via external APIs?	To be discussed on engagement
32.	Are there RAG systems (Retrieval-Augmented Generation) that query internal knowledge bases?	Not at this time
33.	What data sources feed the model (documents, databases, APIs)?	To be discussed on engagement
34.	What was the annual spend for the previous year on this Project?	USAC does not disclose internal budget estimates. Offerors should propose their most competitive pricing based on the requirements
35.	If this is a new Contract, What is the annual Budget for this?	See # 34
36.	Are you open to a hybrid delivery model with a mix of offshore and onshore resources?	All work must be done in the United States
37.	Work will be onsite or remote?	Most technical testing can be remote. Physical testing must be done on site
38.	Can you please give us an extension of 1-2 weeks to submit our proposal?	No
39.	Is this contract intended to be awarded to a single vendor or to multiple vendors?	Single vendor
40.	Who are previous incumbents on this project?	This is a new requirement for a centralized PTaaS offering. Therefore, there is no direct incumbent for this specific service model.

Universal Service Administrative Co.

Q#	Question	Answer
41.	The RFP references annual penetration testing of approximately 16–20 systems while also describing ongoing reporting and ad-hoc testing activities. Could USAC clarify whether the expectation is: One full penetration test per system annually, or A continuous testing model where testing occurs throughout the year? If a continuous model is expected, is there a preferred cadence (e.g., quarterly cycles or staggered testing throughout the year), or would testing primarily occur on demand?	USAC is interested in the most effective approach and open to vendor experience. Each system needs testing annually but no cadence is set. See #53
42.	The RFP references a centralized platform to coordinate testing and deliver results. Could USAC clarify the expected capabilities of this platform? Specifically, should offerors plan to provide a fully featured PTaaS platform (similar to platforms such as HackerOne or other dedicated pentesting portals), or would USAC consider a service-based model where the contractor facilitates testing coordination, reporting, and remediation tracking through integrations with existing systems (e.g., ticketing systems, vulnerability management platforms, or reporting dashboards)?	USAC is interested in an established method and USAC is open to advice and best experience of vendors.
43.	To support vulnerability tracking, reporting, and remediation workflows, could USAC provide guidance on the current platforms used for issue management or security operations (e.g., ServiceNow, Jira, RSA Archer, vulnerability management platforms, or SOAR tools)?	USAC has established processes for vulnerability and POA&M monitoring and use Rapid7, Jira, and Confluence.

Universal Service Administrative Co.

Q#	Question	Answer
44.	The RFP references monthly ad-hoc penetration testing requests. Could USAC provide an estimated volume or typical scope for these activities over the course of a year to assist with planning and pricing?	Ad hoc pen testing requests are primarily for verification of remediation of previous findings with the remainder based on emerging threats or discoveries. Estimate 2 tests per month at about 3 days each for scale.
45.	Should remediation validation (retesting of previously identified vulnerabilities) be assumed as part of the base penetration testing scope, or should this activity be treated as part of the ad-hoc testing requests?	USAC prefers that the vendor reserves work to verify remediations in the estimate of work.
46.	For the three annual social engineering campaigns referenced in the RFP, could USAC provide an approximate size of the user population (employees and contractors) expected to be included in these campaigns?	See #148
47.	For the Wi-Fi and physical access testing at USAC headquarters, should offerors assume a single engagement annually, or multiple exercises throughout the year?	Single engagement annually
48.	The RFP indicates that testing will primarily occur in production-like pre-production environments. Are there any circumstances where production testing may be authorized or requested?	Yes, but rare.
49.	The RFP indicates that testing may involve anonymous users, external users, internal users, and privileged users. Could USAC clarify whether authenticated testing across all user roles is expected for each system, or whether this will vary by system based on risk or architecture?	Testing across roles will vary by system and be risk based.
50.	Kindly confirm the expected penetration testing methodology (Black Box, Grey Box, White Box, or hybrid) for the systems in scope.	USAC is interested in the most effective approach and open to vendor experience.

Universal Service Administrative Co.

Q#	Question	Answer
51.	Please confirm the total number of web applications, APIs, and mobile applications included in the testing scope.	See #2, APIs, no mobile apps 100K IP addresses spread across 201 subnets
52.	The RFP mentions 16–20 systems subject to penetration testing. Kindly confirm the exact number of systems expected to be tested annually.	The number of systems is subject to change so 18 can be an average. Vendors should provide flexibility for scale/scope/complexity as well as count of systems.
53.	Please confirm whether penetration testing for the systems will be conducted annually, quarterly, or on-demand as part of the PTaaS model.	See #45
54.	Kindly confirm the location and architecture of the internal testing environment (on-premise, cloud, or hybrid infrastructure).	Hybrid Infrastructure
55.	Please confirm the approximate number of internal assets (servers, workstations, domain controllers, network devices) that will be included in internal network testing.	~1500 servers, ~730 workstations, 8 Domain controllers, ~200 network devices
56.	Kindly confirm the number of employees or users expected to participate in social engineering campaigns, as well as whether phishing, vishing, and smishing are all required.	Prior phishing campaigns have been enterprise-wide. USAC is open to advice and best experience of vendors.
57.	Please provide additional details on the scope of Wi-Fi testing, including number of access points, network segmentation, and whether rogue access point detection is expected.	See #s 13, 14, 15, 48
58.	Kindly confirm whether penetration testing will be conducted only in pre-production environments or if limited production testing may be permitted.	Pre-Production normally
59.	Please confirm whether testing will include cloud infrastructure components such as AWS, Oracle Cloud, Appian Cloud, and Microsoft 365 configurations.	Yes Including AWS, Appian Cloud, Microsoft 365

Universal Service Administrative Co.

Q#	Question	Answer
60.	The RFP mentions monthly ad-hoc penetration tests. Kindly confirm the expected volume or estimated hours per month for these engagements.	See #45
61.	Kindly confirm whether USAC expects vendors to provide a dedicated PTaaS platform with continuous access and vulnerability tracking, or if traditional periodic penetration testing reports will be sufficient.	USAC is interested in the most effective approach and open to vendor experience. See #143
62.	Who decides the place of performance (e.g. headquarters in DC, virtually, etc.)?	See #202, #83
63.	For internal penetration testing, would you prefer we send a device, or would you prefer to spin up a virtual machine in your infrastructure for testing?	We can spin up a virtual device for infrastructure testing
64.	Typically how long is the training each person must complete?	Less than 1 hour
65.	Will armed guards be present during the physical penetration test? If so, how many?	No
66.	On page 8, a table lists 16 systems that require testing. Are these all web applications?	Yes
67.	Do you expect a separate social engineering test report?	Yes, for each test.
68.	Are we allowed to use compromised credentials for lateral movement during external and internal testing?	Yes
69.	How many in scope external IP Addresses/Range/URLs?	Focus will be on internal. To be discussed on engagement
70.	How many employees will the social engineering campaign include?	Prior phishing campaigns have been enterprise-wide. USAC is open to advice and best experience of vendors.
71.	How many total web applications are included in the scope?	To be discussed on engagement. Generally, from one to 6 per system.

Universal Service Administrative Co.

Q#	Question	Answer
72.	How many mobile applications are included in the scope?	None
73.	Do all in-scope web applications also have mobile applications?	None
74.	On the Excel pricing sheet provided, how are "Small (Low), Medium (Moderate), and Large (High)" System Test Sizes being defined? Are these web applications, mobile/web applications, networks?	Primarily Web applications. See #344, 283
75.	Which locations are in scope for the wireless assessment? (List offices/sites and number of buildings or floors if applicable)	See #11
76.	Approximately how many wireless access points (APs) are deployed in the environment?	About a dozen
77.	What wireless infrastructure vendor(s) are used? (e.g., Cisco, Meraki, Aruba, Ubiquiti, Ruckus, etc.)	See #13
78.	How many SSIDs (wireless networks) are broadcast? Please indicate types if known (Corporate, Guest, IoT, Hidden, etc.).	Two
79.	What authentication methods are used for Wi-Fi access? (WPA2-PSK, WPA3-PSK, WPA2/WPA3 Enterprise – 802.1X, Captive Portal, Open Network)	See #s 13, 14, 15, 48
80.	Is Wi-Fi authentication integrated with a backend identity system? (e.g., Active Directory, RADIUS, Azure AD)	See #s 13, 14, 15, 48 Yes
81.	Are any wireless security controls currently deployed? (e.g., WIDS/WIPS, rogue AP detection, NAC, client isolation)	See #s 13, 14, 15, 48

Universal Service Administrative Co.

Q#	Question	Answer
82.	What testing activities are authorized? (e.g., password cracking attempts, rogue AP/evil twin testing, client attack simulations, captive portal testing)	To be discussed on engagement Generally open to best practices
83.	Will testing require onsite presence, or can some activities be performed remotely?	Only Wi-Fi and physical environment will need a level of onsite presence
84.	Are there any operational constraints or preferred testing windows? (e.g., business hours, after hours, weekends)	Yes, depending on the applications
85.	What are the goals for the facility penetration test?	Verifying that physical access is controlled and not opening penetration opportunities
86.	Would you like us to do Dumpster Diving for the penetration test?	To be discussed on engagement Generally open to best practices
87.	Are you interested in media drops as part of the physical penetration test?	To be discussed on engagement Generally open to best practices
88.	Thoroughness (please choose one from below): ☐ Manual – Our most comprehensive assessment leveraging the best tools, but consisting mainly of manual review (80% manual, 20% tools). ☐ Automated – Appropriate for a lite-weight assessment where budget or time are restricted and manual effort is not desired"	USAC is interested in the most effective approach and open to vendor experience and recommendations. Both methods should be useful.
89.	Environment type (please choose one from below): ☐ Production ☐ Pre-Production (UAT, Test, QA, Staging)	Prod-like test

Universal Service Administrative Co.

Q#	Question	Answer
90.	How will the vendor access the application (please choose one from below): ☐ Direct access ☐ Virtual Desktop Infrastructure (VDI) ☐ Virtual Private Network (VPN) ☐ Other:	USAC is interested in the most effective approach and open to vendor experience and recommendations. VPN and VMs
91.	Type of Testing Requested (please choose one from below): ☐ Application Security Assessments ☐ Mobile Application Security Assessment ☐ Source Code Review ☐ Hybrid Code Review & ASA	Application Security
92.	Is the application and/or its components hosted internally or by a third-party (please choose one from below)? ☐ Internally hosted ☐ Cloud hosted (please explain): ☐ Third-party hosted (please explain):	All variations
93.	Type of application (please select all that apply): ☐ Website ☐ Web Services / API ☐ Mobile Application - iOS ☐ Mobile Application - Android ☐ Thick client (Desktop) Application - Java ☐ Thick client (Desktop) Application - .NET (C#/VB) ☐ Source Code Review ☐ Other:	Web apps primarily

Universal Service Administrative Co.

Q#	Question	Answer
94.	If Mobile, please give the number of platforms in-scope (iOS, Android, etc.) (please select all that apply): ☐ Assessment on Each (iOS, Android, etc.): ☐ Test on One and Validate on the Others:	No mobile apps
95.	Web services (please select all that apply): ☐ SOAP - # of methods ☐ REST - # of methods ☐ WCF - # of methods ☐ Custom - # of methods *Note: please prepare a Postman collection for the vendor to leverage during testing*	USAC is interested in the most effective approach and open to vendor experience and recommendations. To be discussed on engagement
96.	Will documentation, sample requests, or a test harness be made available? ☐ Yes, please explain: ☐ No, please:	Documentation will be available To be discussed on engagement
97.	Size of the application as applicable (please choose one from below): # of Static pages: # of Dynamic pages: # of User Input forms: # of static screens: # mobile views (if applicable): Other, please explain:	To be discussed on engagement Varies by system
98.	For Secure Code Review if desired (Please provide information below): # lines of code: Language(s) of code to be reviewed: Development framework:	this is a PTaaS model covering 16–20 systems of varying complexity (Low, Moderate, High), the specific lines of code (LOC) vary per system and will be disclosed during the individual test coordination phases

Universal Service Administrative Co.

Q#	Question	Answer
99.	Number of Roles for testing? Note: Please be prepared to create two accounts per role in case of account lockout during testing	To be discussed on engagement Varies by system, duplicate roles to prevent lockout can be supported.
100.	Does the application include an accessible administrative interface? ☐ Yes, and in-scope for the assessment ☐ Yes, but out-of-scope for the assessment ☐ No	To be discussed on engagement
101.	Testing Window (please choose one from below): ☐ No restrictions – the vendor will be allowed to test 24/7 during the mutually agreed testing period. ☐ Other: Note: Any testing window restrictions may increase the overall cost	To be discussed on engagement Varies by system, normally planned when access is fully available.
102.	After the report is delivered, would you like to have your remediation efforts validated?	Yes. See #46 and #45
103.	Assessment Location (please choose one from below): ☐ Direct access to a vendor provided virtual machine (OVA) or a shipped physical appliance (SSH/RDP) ☐ Your Virtual Desktop Infrastructure (VDI) ☐ Your Virtual Private Network (VPN) ☐ On-site ☐ Other:	USAC is interested in the most effective approach and open to vendor experience and recommendations. Typically VPN and virtual machine, not On-site

Universal Service Administrative Co.

Q#	Question	Answer
104.	How many live hosts should we expect to see within the scope of the penetration test? (please choose one from below): ☐ less than 500 ☐ 501 – 1,500 ☐ 1,501 – 4,000 ☐ if greater than 4,000, please give an estimate	~1500
105.	Can access be provided such that all in-scope systems are reachable from a single network location?	All systems to test are on USAC's network and accessible on VPN
106.	Is this assessment for the PCI-DSS compliance (requirement 11.3)? ☐ Yes, how many ☐ No	No
107.	What level of information sharing would you like to use during this project? (please choose one from below): ☐ Semi-Blind (provide IP ranges and hostnames only) ☐ Hybrid (Identify target ranges and fill in any gaps prior to the assessment)	USAC is interested in the most effective approach and open to vendor experience and recommendations. Both are possible
108.	What level of evasiveness would you like employed for this engagement? (please choose one from below): ☐ Non-Evasive ☐ Hybrid-Evasive	USAC is interested in the most effective approach and open to vendor experience and recommendations.

Universal Service Administrative Co.

Q#	Question	Answer
109.	How many live hosts should we expect to see within the scope of the penetration test? (please choose one from below): ☐ less than 20 ☐ 21 – 50 ☐ 51 – 100 ☐ 101 – 400 ☐ 401 – 800 ☐ 801 – 1,200	Varies by system. USAC has about 1500 servers
110.	Is social engineering (phishing emails and phone calls) in scope for the external penetration test? (please choose one from below): ☐ No ☐ No, but we would like it as a stand-alone assessment ☐ Yes, please describe:	That is a separate item and anticipate internal tests. USAC is interested in the most effective approach and open to vendor experience and recommendations.
111.	Are any in-scope nodes hosted with a third-party cloud provider? (please choose one from below): ☐ Yes, which: ☐ No	CSPs include Appian, AWS, and Oracle
112.	Are any in-scope assets located outside of the United States? (please choose one from below): ☐ Yes, which: ☐ No	No
113.	Will you be whitelisting the emails and payloads? (please choose one from below): ☐ Will whitelist to better test our people ☐ Will not whitelist to better test our defensive technology	USAC is interested in the most effective approach and open to vendor experience and recommendations. Whitelisting is possible if needed/justified

Universal Service Administrative Co.

Q#	Question	Answer
114.	Would you like your Remote Social Engineering combined with other services selected in this questionnaire or as a stand-alone assessment? (please choose one from below): ☐ Combined with: ☐ As a separate assessment	Social Engineering should be separate assessment(s) and priced separately
115.	Scope. (please choose one from below): ☐ Phone calls ☐ Emails ☐ A combination of both	Both
116.	Goals for the phishing campaign? (please choose one from below): ☐ Only determine who clicked and who reported ☐ Attempt to harvest valid credentials (usernames and passwords) ☐ Develop custom payloads to gain remote access ☐ Other	USAC is interested in the most effective approach and open to vendor experience and recommendations. Be thorough
117.	Would you like the vendor to attempt limited privilege escalation or lateral movement if remote access is achieved?	Yes
118.	What sample size would you like to use for each assessment? Please provide the information below: Phone calls (max 20): Emails:	USAC is interested in the most effective approach and open to vendor experience and recommendations. To be discussed on engagement
119.	Target source. (please choose one from below): ☐ Will provide to vendor ☐ Want the vendor to discover them	USAC is interested in the most effective approach and open to vendor experience and recommendations.

Universal Service Administrative Co.

Q#	Question	Answer
120.	How many different scenarios/campaigns/pretexts would you like us to attempt for each sample of users?	USAC is interested in the most effective approach and open to vendor experience and recommendations. To be discussed on engagement.
121.	What complexity level would you like for each campaign? (please choose one from below): ☐ Easy – Stereotypical scam email (i.e., a prince offers his fortune), many typos, no branding, doesn't address individuals ☐ Medium – One to two grammar errors, can use some branding, doesn't impersonate real internal employees, is impersonal ☐ Challenging – Gloves off, vendor will look to emulate a high-level attacker and mimic reality as much as possible. Emails will be grammatically proper, address recipients personally, and be very realistic	Challenging – please see descriptions in SOW, we anticipate the test to be as challenging as the emerging emulations using AI
122.	How many facilities need to be tested? Note: if more than one, are they all within reasonable (<1 hour) driving distance of each other?	See #12
123.	Brief description of each in-scope location (e.g., two corporate office locations, one data center, a sample of three retail stores, etc.)	See #12
124.	Do you fully own and occupy every facility in-scope? Note: If not, please describe ownership and occupancy	Long term tenant, Boston Properties
125.	After the report is delivered, would you like the vendor to perform testing to validate remediation?	See # 46
126.	Can access be provided such that all in-scope systems are reachable from a single network location?	USAC is interested in the most effective approach and open to vendor experience and recommendations. To be discussed on engagement

Universal Service Administrative Co.

Q#	Question	Answer
127.	Is there an incumbent on this contract? If so, please provide the incumbent name, current contract number, Period of performance, and value of the contract.	Refer to answer 41
128.	Could the government kindly share information on whether there are any pain points or challenges with this contract that we should be aware of while proposing a solution?	USAC does not disclose budgetary information
129.	How many people are currently working on this contract? And what type of people are working.	USAC does not disclose budgetary information
130.	Is there any specific methodology / tools FCC that we should be aware of while proposing a solution?	No
131.	What key performance indicators (KPIs) will define success for this contract?	To be discussed on engagement
132.	Could the government kindly extend the proposal due date by one week?	Due to internal processes, the deadline is not extendable
133.	What challenges or limitations have been experienced with the incumbent organization and their solutions?	Refer to answer 41
134.	The RFP states that 16 systems are currently in scope but up to 20 systems may require testing. For pricing and resource planning, should offerors assume 16 or 20 systems annually?	See #53
135.	If additional systems are added beyond the current 16, will they be treated as new CLINs or part of the base fixed price?	See #53 Depends on the pricing approach of the vendor. For annual core penetration test per system, additional scope may incur additional cost.
136.	Will penetration testing be conducted only in pre-production environments, or will production testing also be required?	Pre-Production normally
137.	Are external penetration tests against internet-facing systems expected?	USAC is interested in the most effective approach and open to vendor experience. Since USAC has a VDP program, this may not be needed.

Universal Service Administrative Co.

Q#	Question	Answer
138.	Will the contractor be responsible for obtaining testing authorization from Cloud Service Providers (AWS, Oracle Cloud, Appian, etc.), or will USAC coordinate this?	USAC will coordinate
139.	What security controls are currently in place (e.g., firewalls, encryption, access management)?	Tested systems will be FISMA moderate authorized.
140.	Can you please provide current number of infrastructure details (Physical Server, Virtual Server, Network Devices etc.	See #56
141.	How much (%) of the infrastructure is in cloud?	About 60-70% of systems are in cloud including Appian and Oracle. Custom systems are mix of premise and AWS.
142.	Are there specific vulnerability severity rating standards required (e.g., CVSS v3.1)?	USAC is interested in the most effective approach and open to vendor experience. CVSS is acceptable.
143.	The RFP mentions a Penetration Testing as a Service (PTaaS) offering. Is a centralized PTaaS platform mandatory, or may vendors provide traditional penetration testing services without a dedicated PTaaS portal?	USAC is interested in the most effective approach and open to vendor experience. PTaaS platform is preferred but not mandatory.
144.	Are there security or FedRAMP requirements for the PTaaS platform itself?	FedRAMP is generally preferred but would anticipate strong security evidence for the platform.
145.	Does USAC require manual testing in addition to automated scanning tools?	USAC is interested in the most effective approach and open to vendor experience.
146.	The RFP states monthly ad hoc penetration tests may occur. What is the estimated number of ad hoc requests per year?	See #45/46
147.	Will retesting of remediated vulnerabilities be counted as ad hoc testing or part of the base scope?	See #45/46
148.	USAC anticipates three social engineering campaigns annually. What is the approximate number of employees or contractors targeted per campaign?	Prior phishing campaigns have been enterprise-wide. USAC is open to advice and best experience of vendors. USAC has approximately 700 target employees and up to 1400 including all contractors.

Universal Service Administrative Co.

Q#	Question	Answer
149.	Will USAC provide employee contact lists and communication channels for social engineering campaigns?	Yes, vendor will work with the USAC SOC and Incident team
150.	For physical penetration testing, how many USAC facilities are included (only HQ or additional locations)?	See #12
151.	Are minimum certifications required for penetration testers (e.g., OSCP, GPEN, CEH)?	We would anticipate only demonstrably skilled testers
152.	Are security clearances required, or only internal background verification?	Internal background is acceptable
153.	The RFP mentions a hybrid onsite policy requiring two days per week in the office. Which contractor roles must comply with this requirement?	This is not required unless the vendor staff needs to be onsite. We have no requirement or expectation for staff to work onsite.
154.	Since USAC systems are FISMA compliant and aligned with NIST SP 800-53 Rev.5, should testing also align with NIST SP 800-115 penetration testing guidance?	Yes
155.	Are there FedRAMP testing restrictions when assessing systems hosted in FedRAMP-authorized cloud environments?	USAC will coordinate with any FedRAMP CSP for access.
156.	Will contractors be required to comply with specific data handling requirements for vulnerability reports containing sensitive information?	Not beyond contractual non-disclosure
157.	Are there encryption standards required for storing or transmitting testing artifacts?	To be discussed on engagement USAC has collaboration approaches for sharing artifacts or reports. Using USAC's network and VPN and VMs should minimize any need for storing any data outside USAC's locations.
158.	Are contractors required to follow specific incident reporting timelines beyond the requirement to report Critical or High findings within one business day?	If an incident or potential incident is identified (not a test finding), then must report to USAC within one hour
159.	Will contractors be required to comply with USAC records retention policies for penetration testing data?	No – all testing records will be stored on USAC collaboration tools or VM, or provided to USAC on conclusion of testing.

Universal Service Administrative Co.

Q#	Question	Answer
160.	Should pricing assume testing of all systems annually, or will testing frequency vary by system?	See #42
161.	Should optional services (social engineering and physical testing) be priced as optional line items or included in the base price?	Please price as optional line items
162.	Should offerors provide separate pricing for each option year, or apply the same pricing as the base year?	Offerors must provide distinct pricing for the base year and all four option years on Attachment 1 (Bid Sheet)
163.	Could the Government consider increasing the page limit for Volume 2 – Technical from 12 to 15 pages and Volume 3 – Past Performance Information from 5 to 10 pages to enable offerors to adequately describe their technical approach and relevant experience?	USAC has considered this request and elects to partially amend the page limits. The revised page limits are as follows: Volume 2 – Technical Approach: Increased from 12 pages to 15 pages. Volume 3 – Past Performance: Remains unchanged at 5 pages.
164.	For each system, can you provide the number of users per user type (anonymous, external, internal non-privileged, internal privileged) to help plan testing effort?	Varies widely depending on the system. To be discussed on engagement
165.	Are user accounts for each user type provisioned by USAC or should the contractor create dummy accounts?	To be discussed on engagement USAC will provide accounts as needed/requested
166.	Are role-based access expectations documented anywhere beyond the System Security Plans (SSPs)?	SSPs or a role-matrix depending on the system
167.	Can USAC provide updated architecture diagrams or high-level network layouts for each system environment?	To be discussed on engagement
168.	For cloud-hosted systems (AWS, Oracle Cloud, Appian, M365), will CSP coordination be handled by USAC or must the contractor initiate coordination?	See #151
169.	For each environment, what access method will be provided (VPN, VDI, jump server, direct connectivity, etc.)?	See #95

Universal Service Administrative Co.

Q#	Question	Answer
170.	Are there any CSP-specific limitations (e.g., AWS penetration test pre-approvals) that USAC is already aware of?	To be discussed on engagement
171.	Does USAC require the contractor to use any specific security testing tools/platforms, or is the contractor free to choose industry-standard toolsets?	USAC is interested in the most effective approach and open to vendor experience and recommendations. Anticipate industry standards, open to emerging tools.
172.	For the PTaaS model, does USAC require integration with any existing platforms (e.g., ticketing systems, dashboards)?	Integration with Jira to generate tickets would be useful
173.	Must the PTaaS platform support multi-factor authentication and SSO via OKTA (as required for cloud services in Section 3.1)?	Yes, but if we need to bypass MFA for test accounts, we can enforce it.
174.	Can USAC confirm that the engagement is strictly testing-focused and does not include continuous monitoring or security operations support? (Since the RFP mentions only testing and reporting.)	Yes
175.	For monthly ad hoc penetration tests, what is the expected average number or volume per year?	See #45
176.	Does USAC require any 24×7 availability during testing windows, especially for critical/high vulnerability retesting or alerts?	No
177.	Are test execution windows restricted to business hours only or can testing occur off-hours for certain systems?	Testing is usually completed during business hours, but may be tested off-hours. Usually settled per system at the engagement pre-test.
178.	Does USAC expect the contractor to include all tool licensing costs (scanners, PTaaS platform, reporting automation) within the fixed price?	USAC anticipates any custom or proprietary tools and platforms to be provided by the contractor. USAC can support provisioning open source and common tools for VMs used for testing.
179.	Are any USAC-owned tools available for contractor use, or must all tooling be contractor-provided?	See #191
180.	Does USAC expect the contractor to perform retesting for all findings, and should retesting be included in the base price?	See #45 and 46

Universal Service Administrative Co.

Q#	Question	Answer
181.	Is there a defined limit on the number of retest cycles per system?	Not defined, but expect one retest per remediation with Ad Hoc costs for repeated or lengthy remediation tests
182.	Does USAC require any consulting support after reports—for example, remediation guidance workshops? (Only remediation instructions are mentioned in deliverables.)	No.
183.	For each system, will USAC provide a documented scope (IP ranges, URLs, APIs, data flows) with each system-specific Penetration Test Plan?	Yes.
184.	Are DoS/DDoS tests permitted on all systems, or must these be excluded unless explicitly approved? (DoS/DDoS is mentioned as part of testing.)	DoS/DDoS tests are generally excluded unless explicitly approved/requested
185.	For application code testing, will code repositories be accessible, or will testing be black-box/grey-box only?	USAC is interested in the most effective approach and open to vendor experience and recommendations. Black/Grey box is expected, so access to code would be unusual.
186.	Can USAC clarify which systems are externally facing and thus require external attack surface enumeration? (Table lists this but may need reconfirmation.)	To be discussed on engagement
187.	Will USAC provide target lists (users, departments) for phishing/vishing/smishing campaigns?	Yes
188.	Is social engineering tests intended to simulate real-world fraud schemes, or must they follow predefined scenarios only?	Real world is requested.
189.	Is USAC expecting contractor hosted phishing infrastructure, or does USAC provide its own?	USAC is interested in the most effective approach and open to vendor experience and recommendations. To be discussed on engagement
190.	For physical access testing, what are the allowed methods (tailgating, badge cloning simulation, desk access, etc.) and what methods are restricted?	USAC is interested in the most effective approach and open to vendor experience and recommendations. To be discussed on engagement
191.	Is after-hours onsite testing permitted at USAC HQ for physical security scenarios?	To be discussed on engagement

Universal Service Administrative Co.

Q#	Question	Answer
192.	For Wi-Fi testing, will USAC provide maps of AP coverage and separate SSIDs for Guest vs. Corporate networks?	To be discussed on engagement
193.	Does USAC have a preferred report format or template, or should the contractor use its standard reporting format?	See #304
194.	Will USAC require CVSS scoring only, or is additional proprietary scoring expected?	See #155
195.	Does USAC require trend analysis across annual tests to show improvements or regressions? (Not explicitly stated.)	Helpful, not necessarily required.
196.	For Significant Alerts (Critical/High), are there any SLAs for remediation guidance beyond the 1-day alert requirement?	No
197.	Does USAC require contractor personnel to have any specific background checks or clearance level beyond the basic visitor form and security training?	No See #165
198.	Is USAC expecting the contractor to provide FedRAMP authorized PTaaS components (if cloud-based)? (Based on cloud requirements in Section 3.1.)	FedRAMP is not a hard requirement for the platform.
199.	Will USAC require onsite presence for kickoff and status meetings, or can all be virtual? (RFP says "may be held virtually" but might need confirmation.)	Onsite presence is not essential.
200.	Would the USAC consider granting an extension to the proposal submission deadline?	Due to internal processes, the deadline is not extendable
201.	May we include additional pages for abbreviations and references, and will those be excluded from the stated page limit?	No those will not be excluded from the page limit.

Universal Service Administrative Co.

Q#	Question	Answer
202.	Regarding Section B.4.A, given that PTaaS is typically a remote-first service, can USAC clarify which 'Contractor Staff' roles are required to meet the 2-day-per-week on-site requirement? Would this apply only to the Account Manager/Key Personnel, or also to the technical testers?	Onsite presence is not required.
203.	Section B.5.A mentions 'intentional poisoning of prompts.' Does USAC have specific LLM-based applications currently in production that are in scope for this, or is this intended for future systems?	To be discussed on engagement Very fast-changing topic and emerging technology that will be deployed to augment our systems over the term of the contract.
204.	Section B.5.B.a.3 states pre-production environments contain 'production-like data.' Will this data be obfuscated/sanitized, or will the testers require specific clearances to handle potentially sensitive program data?	No specific clearances are needed. All data discovered through testing should be retained on USAC provided storage.
205.	Section B.5.C (Deliverable 11) mentions monthly ad hoc reports for remediation or specific targets. Is there a maximum number of ad hoc 'retests' or 'micro-assessments' expected per month for pricing purposes?	See #45
206.	USAC anticipates a PTaaS 'centralized platform.' Does USAC require the platform to integrate directly with their existing ticketing systems (e.g., ServiceNow or JIRA) for automated remediation tracking?	Integration with Jira to generate Vulnerability tickets would be helpful.
207.	Table 1 identifies 'GSS' as a high-complexity system supporting 'all Premise IT, AWS'. To ensure Vendor can accurately scope the network-based portion of this test, can USAC provide a range for the number of live IP addresses, subnets, or VPCs that typically fall under the GSS boundary during an annual assessment?	To be discussed on engagement

Universal Service Administrative Co.

Q#	Question	Answer
208.	For the GSS infrastructure spanning Premises and AWS, will USAC require testing of the site-to-site VPN or Direct Connect links to identify potential lateral movement risks between the cloud and on-premises environments?	USAC is interested in the most effective approach and open to vendor experience and recommendations.
209.	The National Verifier (NV) and UNIFI systems are rated as 'High' complexity. Do these ratings stem from a high number of unique user roles (e.g., external, internal, privileged) or from the underlying architectural complexity, such as numerous API integrations?	NV has significant API connections and very large, though simple, public user base. UNIFi is USAC's core customized financial system that supports upwards of $10B disbursements annually and integrates with the core program systems.
210.	For external-facing systems like E-File, HCBP, and NV, does USAC require a 'Black Box' approach (no prior knowledge) for the external phase, or will documentation like System Security Plans (SSPs) be provided for all phases to support a 'White Box' or 'Gray Box' assessment?	USAC is interested in the most effective approach and open to vendor experience and recommendations. Grey/Black box is primary, and USAC is open to White Box with additional information such as SSP.
211.	Section B.5.B.a.2 states that test environments will have 'production-like configuration and data'. Given the sensitivity of some program data (e.g., PII in the Lifeline program), will this data be masked/obfuscated for the pentest, or must all Vendor researchers meet specific USAC-vetted privacy requirements beyond the standard Rules of Behavior?	Standard security training and rules of behavior should suffice. If additional training is required, USAC will provide along with privileged access RoB.
212.	Since several systems reside on third-party CSPs (Appian, Oracle, AWS), will USAC handle the 'Permission to Test' notifications with these providers, or is the Contractor responsible for coordinating these third-party authorizations?	Yes

Universal Service Administrative Co.

Q#	Question	Answer
213.	Deliverable 11 mentions a 'Monthly Ad Hoc Penetration Test Report'. For fixed-price modeling, can USAC define the expected 'size' of a typical ad hoc request (e.g., a single vulnerability re-test vs. a full assessment of a new system boundary)?	See #45
214.	Regarding the 16 to 20 systems identified in Table 1, could USAC provide an estimated number of IP Addresses, dynamic pages, API endpoints for a representative 'Low', 'Moderate', and 'High' complexity application?	To be discussed on engagement
215.	For systems where network penetration testing is required, can USAC provide the appropriate number of live IP addresses and/or CIDR blocks?	To be discussed on engagement
216.	Several systems reside on Appian Cloud, AWS, Oracle Cloud, and ServiceNow (SNow). Will USAC handle all necessary penetration testing authorizations with these Cloud Service Providers (CSPs), or is the Contractor expected to coordinate this?	Yes
217.	Referring to "Core Penetration Testing... The Contractor will propose an approach that supports testing for USAC's mission systems...". Does USAC have an anticipated duration (e.g., 5 days, 2 weeks, etc) for the penetration tests of the High, Moderate, and Low complexity systems?	USAC is interested in the most effective approach and open to vendor experience and recommendations. Prior allocations for penetration testing have been successful at 2 week, 3 week, and 4 week test duration. USAC is not prescribing specific length of test time.
218.	Referring to "USAC anticipates three corporate-level campaigns annually, working closely with the Contractor to organize, support, and assess results." For the three (3) annual Social Engineering campaigns, approximately how many USAC employees and contractors will be targeted in these exercises?	USAC is interested in the most effective approach and open to vendor experience and recommendations. USAC has targeted all employees in phishing tests – approximately 700.

Universal Service Administrative Co.

Q#	Question	Answer
219.	Referring to "Contractor shall not use, implement, build, or deploy AI tools, services, or code of any type without prior written approval from USAC." If a Contractor utilizes a proprietary, closed-system AI engine solely for internal backend operations (such as matching tester skillsets to target requirements) that does not ingest USAC Data or PII, does this require explicit pre-authorization under this clause?	USAC will facilitate approvals for any proposed use of AI, so will anticipate details from the contractor to support approval.
220.	In the event of ad hoc requirements for testing, New applications, global events (e.g., Log4J, React4Shell) requiring threat hunting/identification of critical vulnerabilities, application changing boundaries- How does USAC want vendors to address this in their response?	USAC expects pricing and potential scalability of ad hoc testing that could be required in the case of an emerging incident.
221.	Referring to Deliverable 11, what is the estimated historical or anticipated volume of ad hoc test requests?	See #45, #233
222.	Referring to Optional Physical Environment Testing, for Wireless Testing, what is the anticipated number of SSIDs and WAPs to be tested? How many different configurations and types of equipment exist?	See #13
223.	Do any of the moderate/ higher complexity systems have more than 3- 4 user roles or have multiple applications embedded inside of them that will require additional testing?	The more complex systems have more roles and may have multiple applications depending on the design. The configurations and targets would be discussed when engaging to prepare for testing. All roles do not need to be tested in favor of testing a more critical or risky roles.
224.	Is the PTaaS Platform required to be FedRAMP Moderate Authorized?	FedRAMP Moderate is preferred but not essential.

Universal Service Administrative Co.

Q#	Question	Answer
225.	Should offerors assume that all 16 current systems will be tested annually in the base and each option year, with pricing scalable only if the count increases above 16 up to 20or should offerors price against a variable annual testing volume within the full 16–20 range?	See #53 and pricing by test categorical size or test day will be helpful
226.	For systems added due to boundary changes or newly deployed systems, does USAC expect offerors to propose a unit-rate or complexity-based pricing model for those incremental systems in Attachment 1?	Yes.
227.	For the required monthly ad hoc testing support, can USAC clarify the anticipated annual volume number of requests, estimated testing hours, or expected test targets per month so offerors can price fixed-fee support more accurately?	See #45
228.	For retesting of remediated findings, should offerors assume retesting is included within each annual system test price, or does USAC intend retesting to be priced separately under ad hoc testing or another line item?	Expect one retest per remediation with Ad Hoc costs for repeated or lengthy remediation tests
229.	Can USAC clarify the minimum required platform capabilities such as role-based access, workflow/tasking, evidence management, dashboarding, downloadable reports, API integration, SSO, or ticket export?	USAC is interested in the most effective approach and open to vendor experience and recommendations.

Universal Service Administrative Co.

Q#	Question	Answer
230.	If contractor personnel use USAC-issued technology and USAC-approved environments for storage and sharing of USAC documents, may the contractor still use a separate PTaaS coordination portal for scheduling, findings workflow, and reporting metadata provided no USAC documents or confidential content are stored outside approved locations?	Yes
231.	Can USAC clarify whether the centralized PTaaS platform is intended to be: (a) contractor-hosted, (b) USAC-hosted, or (c) operated only through USAC-issued technology and collaboration tools?	USAC is interested in the most effective approach and open to vendor experience and recommendations. Contractor hosted is anticipated.
232.	Section B references "Application Code testing" for session management. Can USAC clarify whether this requirement is limited to dynamic application security testing of runtime behavior, or whether USAC expects source code review / secure code analysis as part of the core annual test scope?	Source code review/analysis is not requested.
233.	For the listed "resistance to DoS/DDoS," should offerors assume this means assessment of resilience, architecture, and control effectiveness or does USAC expect controlled live denial-of-service simulation in production-like environments?	Live DoS/DDoS is not requested.
234.	Can USAC provide any expected distribution of test depth by system complexity level so offerors can align staffing assumptions across low, moderate, and high complexity systems?	The higher complexity systems will need more in-depth testing.
235.	For the four user perspectives listed, should offerors assume USAC will provide representative accounts and roles for each test scenario, including privileged roles where applicable?	Yes.

Universal Service Administrative Co.

Q#	Question	Answer
236.	For the optional social engineering scope, are offerors expected to price three annual campaigns as a standing commitment in every contract year, or should pricing be structured as optional task-based exercises that USAC may elect to order?	Please price for every contract year.
237.	For the optional physical environment testing, should offerors assume a single annual HQ exercise covering both Wi-Fi and physical access, or is separate pricing expected for each component?	Yes, one exercise per year.
238.	For AI-assisted social engineering simulation and AI-related malicious action testing, does USAC have any boundaries, approval workflows, or prohibited techniques that offerors should reflect in their technical approach?	USAC is interested in the most effective approach and open to vendor experience and recommendations.
239.	Because key personnel are required to be named in the proposal, would USAC permit offerors to identify contingent hires who have signed letters of commitment effective upon award or must all named key personnel already be on staff at time of proposal submission?	Yes, USAC will accept contingent hires for Key Personnel roles. Offerors must include a signed Letter of Commitment for any named individual not currently employed by the firm. All proposed Key Personnel must be fully available to begin performance on the Contract Effective Date
240.	Beyond the Contract Engagement Manager, does USAC expect named resumes for leads covering application penetration testing, network/infrastructure testing, social engineering, and physical testing if those services are proposed?	Need at least primary technical lead, additional skilled individuals are helpful.
241.	Will qualified personnel with disabilities be proposed in any role consistent with the PWS capable to do the work?	Yes. USAC is an equal opportunity employer and encourages its Contractors to maintain inclusive hiring practices. Qualified personnel with disabilities are eligible to be proposed for any role described in the PWS, provided they meet the specific technical requirements, security clearance criteria, and "Key Personnel" qualifications (Section 6) necessary to perform the required services

Universal Service Administrative Co.

Q#	Question	Answer
242.	Can USAC clarify whether privacy and security requirements apply only to contractor-managed systems that store, process, or transmit USAC data versus tools used solely on USAC-issued devices and USAC-approved environments?	Yes, correct.
243.	If an offeror uses a FedRAMP-authorized cloud environment for internal workflow support but stores final USAC work products only in USAC-approved locations, would that satisfy USAC's intent regarding contractor IT controls and document handling?	Yes
244.	Since USAC may reject testing or reports and require re-testing or revisions at contractor cost, can USAC clarify the acceptance criteria for test plans, reports, and re-test sufficiency to ensure offerors can price the risk appropriately?	Rejection, if it happens, will be fact based and related to deliverable accuracy, validity, comprehensiveness, completeness, and appropriateness of communications.
245.	Can USAC clarify whether there is an expected annual testing schedule or sequencing for the core systems, so offerors can better estimate staffing peaks, lead times, and surge requirements?	See #42, #53 For practicality, we avoid more than three active concurrent tests when scheduling.
246.	RFP Document Section B, #1 Overview, Paragraph 1, Page 5: Will USAC please provide additional details on fraud risk requirements specific to Penetration Testing for purposes of scoping (e.g., explanation of the types or use-cases of fraud USAC anticipates or may experience)?	USAC is interested in any vulnerability that may open the door for fraud or fraud risk versus the traditional security and privacy risks.
247.	RFP Document Section B, #10 USAC Technology and Email Use, Paragraph 1, Page 13: Will USAC please confirm if the contractor will be allowed to install additional penetration testing tools on USAC-issued technology to assist in penetration testing activities (e.g., Metasploit, Wireshark, AI-based tooling, etc.)	See #171

Universal Service Administrative Co.

Q#	Question	Answer
248.	RFP Document Section B, #10 USAC Technology and Email Use, Paragraph 2, Page 13: For external facing systems in scope of testing, may the contractor use tools and systems outside of USAC-issued technology (i.e., Contractor laptops or tools) to assess the security posture?	USAC is interested in the most effective approach and open to vendor experience and recommendations.
249.	RFP Document Section B, #7 Meetings, Paragraph 2, Page 12:. Meetings indicate Kick-off meeting no later than ten (10) workdays after any contract award, however Section C. Deliverables #1 indicates submission within five (5) business days of contract award. Will USAC clarify to confirm this is intended to be ten (10) business days, as outlined in the deliverable table?	USAC confirms that the kick-off meeting is intended to be held no later than ten (10) business days after contract award, consistent with the Deliverables table. To resolve the discrepancy between Section B and Section C, a redlined RFP will be posted to provide formal clarification and ensure all sections are aligned
250.	RFP Document Section B, #4 Place of Performance, Paragraph A, Page 5: Would USAC consider allowing exceptions to the in-person requirement, so that contractors may staff the project with personnel that are not DC-based?	See #37 and #83
251.	RFP Document Section E, #6 Proposal Content, Paragraph E.2, Page 57: Would USAC consider removing the cover page and the table of contents page from the page count requirements?	Please note that a Table of Contents (TC) is not required for this submission and will be counted toward the page limit. However, to accommodate comprehensive responses, USAC has increased the page limit for the Technical Proposal to 15 pages
252.	RFP Document Section B, #C Deliverables, Paragraph C, Page 10: Can USAC confirm the maximum number of penetration tests that they expect to run concurrently?	See #245
253.	RFP Document Section B, #C Deliverables, Paragraph C, Page 10: Can USAC confirm the expected duration for each Penetration Test based on Pentration Testing complexity?	See #217

Universal Service Administrative Co.

Q#	Question	Answer
254.	Attachment 1 Bid Sheet, Table Titel “Daily Rate”: Can USAC confirm that contractors should provide "Total Price" versus "Daily Rate"?	Yes, totals are needed.
255.	RFP Document Section B, #6 Systems Subject to Penetration Testing, Table 1, Page 8: Will physical access be required to test on premises applications or will remote access be provided such as a VPN for testing?	All systems and applications are accessible by VPN for remote access.
256.	RFP Document Section B, B. Social Engineering Testing, Paragraph 3, Page 9: Approximately how many users does USAC believe will be targeted for each Social Engineering test?	See #18, #46, #148
257.	Is there an incumbent on this contract? If so, please specify.	See #41
258.	Does this effort have a funded budget allocated? If so, what is the estimated ceiling value?	See #34
259.	Can the USAC confirm Attachment 2 - Confidentiality Agreement will be submitted separately outside of Volumes 1-4?	Yes. USAC Confidentially Agreement can be submitted separately.
260.	Can the contractor propose the schedule or is there a fixed date all assessments need to be completed by?	See #53, #225, #41
261.	The RFP states “*Contractor shall propose additional Key Personnel such as engineers, consultants and/or IT lead, who will be key to providing the Services/Deliverables described in the RFP.*” Can USAC confirm that resumes do not need to be supplied for ALL personnel working on this program, just personnel that the Offeror deems key beside the Contract Engagement Manager?	Yes.

Universal Service Administrative Co.

Q#	Question	Answer
262.	Can the USAC confirm the USAC STANDARD TERMS AND CONDITIONS PRIVACY AND SECURITY ADDENDUM is to be completed post award?	USAC requires that both the USAC Standard Terms and Conditions and the Privacy and Security Addendum be reviewed and any changes or exceptions must submit as part of the Offeror's proposal.
263.	Can the USAC confirm that all personnel on the program are not key and that Key Personnel in addition to the Contract Engagement Manager is at the discretion of the offeror?	See #261
264.	The RFP states "*For each past performance, provide a description of the relevant performance for each project discussed. A past performance description will consist of: (i) an overview of the engagement, (ii) a description of the scope of work performed, (iii) its relevance to this effort, and (iv) the results achieved. This is the time to identify any unique characteristics of the project, problems encountered, and corrective actions taken. Each overview shall not exceed one (1) page.*" Can USAC clarify if a past performance description as a whole shall not exceed one (1) page or just the overview of the engagement is not to exceed one (1) page?	Each past performance description as a whole shall not exceed one (1) page. The total page limit for the Experience and Past Performance Information is 5 pages.
265.	Can the USAC confirm that if they are unable to contact the past performance references, that they will then reach out to the OFFEROR's contacts identified on the proposal with a PPQ that the Offeror will then send to the past performance reference to be completed by the specified date in the transmittal?	USAC cannot confirm this process. It is the sole responsibility of the Offeror to provide accurate and reachable contact information for all past performance references. USAC reserves the right to evaluate proposals based only on the information provided and is not obligated to notify Offerors or provide additional time if a reference is unresponsive. Offerors are strongly encouraged to verify the availability of their references prior to proposal submission

Universal Service Administrative Co.

Q#	Question	Answer
266.	If the offeror's past performance is done as a subcontractor, will the USAC accept a PPQ from the prime on that contract?	Yes, USAC will accept a Past Performance Questionnaire (PPQ) from a prime contractor for work performed by the Offeror as a subcontractor. When submitting such references, the Offeror must clearly identify their role on the project and ensure the PPQ specifically evaluates the scope of work they performed, rather than the performance of the prime contractor as a whole
267.	Will USAC allow Commercial contracts to be utilized as past performance experience examples even if they do not have official contract numbers?	USAC will allow commercial contracts to be utilized as past performance examples. While an official federal contract number is not required for commercial entries, the Offeror must provide a unique identifier (such as a Purchase Order number, internal project code, or specific contract title) to allow USAC to accurately track and verify the reference.
268.	Can the USAC confirm that Volume 4 will just consist of a cover page and Attachment 1 - Bid Sheet?	Yes. That is correct
269.	The RFP states "*The proposed price must be fully loaded and must include wages*" Can the USAC clarify if wages are referring to the Labor Category hourly amount for a personnel or the actual salaried wage of the personnel being proposed?	USAC clarifies that 'wages' in the context of a fully loaded price refers to the Labor Category hourly rate proposed for the services, not the internal salaried wage of individual personnel. The proposed rate must be all-inclusive, covering the base labor rate plus all applicable 'burden' elements, including fringe benefits, overhead, General and Administrative (G&A) expenses, and profit
270.	Can the USAC confirm that Volume 4's 4 page limit would consist of a cover page (1 page), tab 1 - summary (1 page), and tab 2- alt-proposed price (2 pages)?	Yes. That is correct
271.	How is the USAC determining a page in excel? Should the Offeror use the print feature to determine a page?	The page limit for Volume 4 (Price) applies specifically to the Price Narrative (PDF). There is no page limit for attachment 1 - bid sheet (Excel workbook). However, the Offeror must ensure the file is formatted for clear readability and is 'print-ready' using standard 8.5" x 11" layout settings. USAC will not use the print feature to enforce a page count on Excel files, but all data, formulas, and pricing tables must be easily accessible for evaluation

Universal Service Administrative Co.

Q#	Question	Answer
272.	The RFP states "*Offeror's past performance will be evaluated based on Offeror's discussion of its past performance for similar efforts, information obtained from past performance references (including detailed references for Offeror's proposed teaming partner(s) and/or subcontractor(s), as applicable),*" Can the USAC clarify how proposed teaming partner(s) and/or subcontractor(s) references would be evaluated and/or obtained?	USAC evaluates the past performance of proposed teaming partners and subcontractors in the same manner as the prime Offeror. These references should be submitted within Volume 3 (Experience and Past Performance) and must include the same required details: (i) engagement overview, (ii) scope of work, (iii) relevance to this RFP, and (iv) results achieved. USAC will obtain and verify these references using the contact information provided in the proposal or through a Past Performance Questionnaire (PPQ), if applicable
273.	Can we include Table of contents, if yes does it count towards page limit	A Table of Contents is permitted but not required. Please note that if included, these pages will count toward the total page limit for each volume.
274.	Do we have to include T&C or just give acknowledgement statement for Terms and Conditions?	Please include the acknowledgment.
275.	5-page limit for pricing narrative and not for bid Sheet? Please clarify	Bid Sheet is Attachment 1 and does not count toward page limitation of Volume 4.
276.	We request to increase page limit from 12 to 20 if possible	Refer to answer 176
277.	We request to increase submission Deadline by a week?	Refer to answer 145
278.	What is estimated budget for this requirement? And Who is the incumbent on this work right now?	USAC does not disclose internal budget estimates. Offerors should propose their most competitive pricing based on the requirements. This is a new requirement for a centralized PTaaS offering. Therefore, there is no direct incumbent for this specific service model.
279.	What challenges agency is facing?	Compliance.
280.	Would USAC allow the vendor you select to use their own remote testing appliance?	See #171

Universal Service Administrative Co.

Q#	Question	Answer
281.	You state that the proposal is to be submitted in the form of one electronic copy but then state that each volume is to be submitted as a separate attachment – please confirm how you want our proposal volumes to be submitted.	We confirm that your proposal should be submitted via a single email. The submission must include four (4) separate PDF attachments, as follows: • Volume 1: Company Information • Volume 2: Technical Approach • Volume 3: Experience and Past Performance • Volume 4: Price
282.	Will a consultant be required to be physically present in the USAC office at least two days per week?	#153
283.	How is a small/medium/large test defined? May we set the parameters?	Yes
284.	Does USAC require a Contractor hosted Penetration Testing as a Service (PTaaS) platform to obtain a FISMA Authority to Operate (ATO) in addition to being hosted on a FedRAMP Moderate–authorized cloud service, or is FedRAMP authorization of the hosting environment sufficient?	FedRAMP authorization of a Cloud Service Offering (CSP) for the cloud would be compliant. Simply operating on an Infrastructure-as-a-Service (IaaS) platform does not comply with FedRAMP requirements for an offered service.
285.	For the systems identified in Table 1, should Offerors assume that all systems will be tested annually, or will USAC apply a risk based rotation with variable testing frequency by system?	See #52,
286.	Are there any constraints on concurrent penetration testing, such as limits on the number of systems that may be tested simultaneously?	See #245
287.	Does USAC have any preferred or restricted testing windows (e.g., business hours versus off hours/weekends), particularly for mission-critical or externally facing systems?	See #84, #177

Universal Service Administrative Co.

Q#	Question	Answer
288.	Will the preproduction environments used for penetration testing contain masked/anonymized data, production derived data, or synthetic data, and are there any restrictions on PII within those environments?	Depends on the system and set-up per application and database. To be discussed on engagement. See #211, #219
289.	Does USAC require or prefer a specific vulnerability severity scoring model (e.g., CVSS v3.1 with defined thresholds) for penetration test reporting and POA&M alignment?	See #142
290.	How many rounds of remediation retesting should Offerors assume per system or per finding, and should remediation retests be included within the firm-fixed price or treated as ad-hoc testing?	See #46 and #45
291.	Does USAC have standard templates for penetration test plans, reports, or monthly status reports, or should Offerors propose their own formats for approval?	Offers should propose content for each, USAC is flexible on format
292.	For Contractor hosted IT and cloud services, will USAC accept existing FedRAMP authorization packages, ISO 27001 certifications, and SOC 2 Type II reports as sufficient evidence, or are additional USAC specific assessments required?	No other specific assessments.
293.	The Privacy & Security Addendum restricts the use of artificial intelligence. Would USAC permit AI assisted tooling for internal test orchestration or draft report generation, provided no USAC data is used for model training and all outputs are human reviewed?	Yes, AI is requested where viable and constrained. USAC is interested in the most effective approach and open to vendor experience.

Universal Service Administrative Co.

Q#	Question	Answer
294.	Following contract expiration or termination, what are the required data retention and destruction timelines for penetration testing artifacts such as raw scan data, logs, screenshots, and exploit code?	Upon contract expiration or termination, the Contractor must follow specific protocols for all USAC Data, including penetration testing artifacts (scans, logs, screenshots, and exploit code): 1. Retention Period: The Contractor must retain all USAC data and documents in accordance with USAC's record retention policy (p. 14). This typically requires records to be maintained for at least six (6) years after final payment, unless the data is part of a federal system of record subject to National Archives and Records Administration (NARA) schedules (p. 24). 2. Destruction Requirement: Promptly upon expiration, the Contractor must, at USAC's direction, return or destroy all USAC Data at no additional cost (p. 24). Destruction Methods: 1. Electronic Copies: Must be destroyed according to NIST SP 800-88 Rev. 1 guidelines (p. 24). 2. Hard Copies: Must be destroyed by burning, pulping, shredding, or macerating (p. 24). 3. Verification: Contractor must provide a written certificate to USAC confirming all data has been destroyed (p. 24)
295.	May Offerors include technical attachments (e.g., redacted sample reports or architectures) outside the page limits, or must all technical content other than resumes be contained within the stated limits?	Refer to answer 214
296.	Does USAC anticipate changes in system count, hosting environment, or scope during the option years that Offerors should consider when proposing multi-year fixed pricing?	Changes are inevitable, even within a contract year. Please propose pricing that supports adapting to changes such as new systems, realigned security boundaries, decommissioning systems, and urgent tests to support emerging issues.

Universal Service Administrative Co.

Q#	Question	Answer
297.	Are there any required or preferred professional certifications (e.g., OSCP, GXPN, CISSP) for Key Personnel beyond background checks?	No. USAC is interested in the most effective approach and open to vendor experience and recommendations.
298.	Does USAC utilize Appian internally for application development and administration, or is Appian primarily consumed by USAC after applications have been developed and deployed by contractors?	USAC is a major developer and maintainer of Appian applications developed on the Appian FedRAMP PaaS CSP.
299.	Does Appian within the USAC environment integrate with internal identity providers such as on-premises Active Directory, or exclusively with cloud based identity services?	Yes, AD and Okta.
300.	The RFP references multiple cloud environments but does not list Microsoft Azure. Should Offerors assume Azure hosted systems are out of scope, or may Azure environments be included in penetration testing during the contract term?	No Azure hosted systems.
301.	Is source code and supporting documentation generally available for API and web application penetration testing? If so, can USAC provide an approximate percentage of systems for which source code and documentation will be provided?	To be discussed on engagement – varies by system
302.	The RFP states that travel is not reimbursable, while physical testing is an optional service. Will USAC allow an exception for travel costs specifically associated with approved physical penetration testing activities?	USAC will not allow exceptions for travel costs, even for optional physical penetration testing activities. As stated in the RFP, the proposed price must be 'fully loaded' and inclusive of all direct and indirect costs, including travel. Offerors should factor any anticipated travel expenses required to perform physical testing into their firm-fixed-price proposal for that optional service item
303.	Does USAC have standing approval from third party cloud providers for the requested activities?	No. To be discussed on engagement per system. See #212

Universal Service Administrative Co.

Q#	Question	Answer
304.	Does USAC own and control all locations in scope, or are any facilities operated, leased, or managed by third parties that require additional approvals, rules of engagement, or coordination prior to testing?	See #212. USAC leases physical building for HQ offices.
305.	PTaaS platform expectations: USAC "anticipates a PTaaS offering…through a centralized platform." Please confirm (a) whether a multi-tenant SaaS portal is acceptable, and (b) whether FedRAMP Moderate authorization is required for the PTaaS portal itself.	(a) Yes; (b) Preferred
306.	Production vs. preproduction: Section B.5.B.i–ii specify testing in "preproduction environments with production like data". Will any limited production testing be permitted (e.g., auth/session handling, WAF rules validation) under strict ROE, or is all testing prohibited in production? Please also define any prohibited test techniques.	To be discussed on engagement. Anything in production will be severely limited.
307.	Campaign design: USAC anticipates three corporate level campaigns annually. Does USAC prefer (a) baseline + targeted waves, (b) role-based scenarios (e.g., finance, IT, execs), or (c) a mix aligned to current fraud scenarios? Any exclusions (e.g., legal, HR, Board)?	USAC is interested in the most effective approach and open to vendor experience. A risk-based mix aligned with current/emerging threat posture and fraud schemes is preferable.
308.	Awareness integration: Should campaigns include just in time training/landing pages, and does USAC have existing LMS integration requirements for training completion data?	The RFP is not requesting training.
309.	Phone/SMS originations: Are there caller ID/SMS masking constraints for vishing/smishing (e.g., prohibitions on spoofing internal numbers/domains)?	No.

Universal Service Administrative Co.

Q#	Question	Answer
310.	AI assisted pretexting: RFP references AI use by adversaries. May we employ AI generated voice, text, or deepfake content for realism, or are these restricted under USAC's AI policy (Section 3.3)? Please clarify guardrails.	USAC is interested in the most effective approach and open to vendor experience. To be discussed upon engagement.
311.	Is it acceptable to USAC for the contractor to propose an on-premises solution, or is there a preference for a CSP-based solution?	USAC is interested in the most effective approach and open to vendor experience.
312.	Would USAC consider changing the minimum FedRamp authorization from Moderate to Low, considering this engagement is in USAC pre-production system environments?	Yes.
313.	In the RFP doc, there are 16 systems in-scope. Of those 16, does USAC control the software development of any of the in-scope applications?	All.
314.	What are the crown jewels for each of the in-scope systems?	To be discussed on engagement
315.	Are there any specific attack paths that you are concerned about in any of the systems/applications?	To be discussed on engagement Current POA&Ms and vulnerability data will be available.
316.	Are any of the in-scope web applications considered to be B2B multi-tenant applications?	To be discussed on engagement No multi-tenant apps
317.	If yes, how many and which applications are considered B2B?	To be discussed on engagement
318.	What information would be most detrimental for an attacker to get to through Social Engineering?	To be discussed on engagement
319.	Are there any specific pretexts you would like us to utilize against your employees?	To be discussed on engagement
320.	Are there specific pretexts you would like us to avoid?	To be discussed on engagement
321.	Number of employees to be emailed	See #148
322.	Would you like us to Harvest Credentials, get users to run malicious code, or both?	To be discussed on engagement

Universal Service Administrative Co.

Q#	Question	Answer
323.	Does USAC have employees that handle help desk calls?	USAC has an internal IT service desk, operates two programmatic help desks for external users.
324.	How many employees are going to be in-scope (we usually scope vishing for 20 employees)?	~700 To be discussed on engagement
325.	Is the use of deep voice clone in-scope?	yes
326.	How many employees are going to be in-scope?	~700
327.	How many office locations does USAC have? Are all in scope?	Only One at Metro center
328.	What type(s) of business are conducted at the location?	Management, development, operations
329.	What are the primary objectives to reach?	To be discussed on engagement
330.	What are the active business hours?	9:00 AM to 6:00 PM Monday to Friday
331.	Will we receive floorplans of the building?	Yes
332.	Are there any areas that are explicitly off limits?	To be discussed on engagement
333.	Are daytime and nighttime attempts in-scope?	Yes
334.	Is there armed security guards?	Yes
335.	If yes, what are their working hours?	24x7
336.	Is there an alarm system in place? Which brand/type is it and when is it active?	Yes - To be discussed on engagement
337.	What triggers an alarm (motion, glass break)?	To be discussed on engagement
338.	Do you have surveillance cameras? If so, are they live monitored?	Yes
339.	Who is monitoring the alarm system/cameras? Who is the first person in the call tree?	To be discussed on engagement
340.	How many SSIDs are in-scope?	Two
341.	Are all in-scope SSIDs going to be reachable from one location?	Yes

Universal Service Administrative Co.

Q#	Question	Answer
342.	Do you want our team in person two days a week for this project per the statement below? A. All required Services (as defined in Section C.1.U) under the awarded Contract must be performed within the United States at either USAC's headquarters at 700 12th Street NW, Suite 900, Washington, DC 20005 ("USAC Headquarters"), virtually, or such other location as USAC may approve in its sole discretion. Presently, USAC has a hybrid work approach requiring Contractor Staff (as defined in Section C.1.G) to be in the USAC office at least 2 days per week. Contractors that are required to report in person must reserve their workspaces in designated areas in advance using USAC's hoteling system. G. "Contractor Staff" means Contractor's employees, subcontractors, consultants, and agents used to provide Services and/or create Deliverables under this Contract, including, but not limited to, Key Personnel. "Contractor Staff" also includes the entity that employs Contractor's employees, subcontractors, consultants, and agents in all cases except where the context clearly references only individuals.	See #153
343.	Are there any mobile applications or client applications? If so, what type? (iOS, Android, Windows)	No mobile or client applications.

Universal Service Administrative Co.

Q#	Question	Answer
344.	BreachLock prices our web application pentests based on size of application according to dynamic pages (e.g. Up to 20 Dynamic Pages, Up to 50 Dynamic Pages). A. Can USAC provide BreachLock the estimates of dynamic pages for each application in accordance with the following scale? • Small: Up to 50 Dynamic Pages • Medium: Up to 100 Dynamic Pages • Large: Up to 200 Dynamic Pages • X-Large: 200+ Dynamic Pages Or B. Can BreachLock assume that the table's complexity scores align to the following sizes? • Low complexity: Up to 50 Dynamic Pages • Moderate complexity: Up to 100 Dynamic Pages • High complexity: Up to 200 Dynamic Pages	You may assume B. works in general

Universal Service Administrative Co.

Q#	Question	Answer
345.	Under paragraph B. Summary of Service Capabilities Required, the Core Penetration Testing services outline Core Systems as 16-20 systems, but also later references Internal Network Scanning under B.4.a. A. Are Internal Network and External Network Pentests required for your Infrastructure-as-a-Service (SaaS) environment(s)? If yes, what is the estimated number of internal IPs/hosts in scope for testing and how many different segments of the virtual network are there, and how many public IPs/FQDNs would be in scope at network-layer?	See #5,
346.	FISMA compliant systems and FedRAMP authorized Cloud Service Providers (CSPs) are mentioned in B.a.1. Does the chosen Penetration Testing as a Service (PTaaS) vendor for this RFP need to be FedRAMP certified, or will testing in accordance with FedRAMP requirements and NIST SP 800-53 align instead?	See #144, #224
347.	BreachLock prices our Social Engineering engagements (vishing, phishing) based on quantity of employees/targets per campaign. Under B.b Social Engineering Testing (Optional), there not a specific quantity of employees/targets listed. A. Is USAC's intent to target all employees throughout the three annual campaigns, or will the campaigns be contained to smaller groups of targets? If smaller groups of targets, how many targets per campaign?	See #18, #56, #70, #110, #116, #148, #187, #218
348.	What approximate budget ranges would be allocated to the 16-20 FISMA engagements, as well as social engineering and physical testing?	USAC does not disclose internal budget estimates. Offerors should propose their most competitive pricing based on the requirements

Universal Service Administrative Co.

Q#	Question	Answer
349.	Can reports be separated by methodology type or consolidated into a single report for each FISMA engagement?	To be discussed on engagement
350.	For social engineering, when using a sampling approach approximately how many users would be targeted out of the 1000+?	USAC is interested in the most effective approach and open to vendor experience.
351.	What types of services/infrastructure can be found within the CSPs (specifically AWS/Oracle)?	To be discussed on engagement. Oracle is used for the ERM (Finance) solution. AWS is cloud infrastructure for development/operations of business solutions.
352.	When evaluating cloud environments, would the approach be to review the configuration level or to test the network layering as well?	Mostly at the network layering level
353.	Regarding pentest complexity (low, moderate, high), how many pentesting days have these applications typically been allocated?	Most Penetration Tests are completed in 3 to 4 weeks for annual testing of a system.
354.	Are external surfaces of each FISMA application considered in-scope? (ie. Associated public IPs or FQDNs)	Generally, no. To be discussed on engagement.
355.	For testing of USAC's internal networks, approximately how many IPs or hosts are considered active?	See #5
356.	For the applications that consider API testing in scope, do said APIs support the application's front-end content or are they callable directly through token access?	Directly callable from established counterparties
357.	Would USAC accept a vendor who is fully remote and would not be on-site with them for an ongoing cadence?	Yes
358.	Do all test contractors require USAC onboarding?	Yes

Universal Service Administrative Co.

Can you provide asset counts for the following?

Answer: To be discussed on engagement with each system for testing during or after contract award.

Systems	Pen Test complexity	Virtual Host Count:	Physical Host Count:	Database Count:	Router/Switch Count:	Firewall Count:	Web Application Count
AppCloud	Moderate						
CAMP	Low						
EDS	Moderate						
E-File	Moderate						
FDT	Moderate						
FOS	Moderate						
GSS	High						
HC Apps	Low						
HCBP	Moderate						
HCLI 2.0	Moderate						
NLAD	High						
NV	High						
RHC	Low						
RPA	Low						
S&L	Low						
UNIFi	High						