Universal Service Administrative Co.

Universal Service Administrative Co. (USAC)

IT-25-188 – Penetration Testing as a Services

Questions & Answers

Q#	Question	Answer
1.	Does USAC require an existing PTaaS platform, or is USAC open to a provider using a hybrid model (custom dashboards + manual testing)?	USAC is interested in existing PTaaS platforms only.
2.	Does USAC require continuous testing, or only on-demand testing per boundary?	USAC is interested in what is available or offered/recommended.
3.	What ITSM/SOC tools does PTaaS need to integrate with (ServiceNow, JIRAS, Splunk, Sentinel, Archer, etc.)?	Jira (Cloud) for ticketing. USAC uses Splunk for SIEM. Rapid7 for vulnerability.
4.	What level of user access is required (employees, contractors, BPO vendors)?	Employees, contractors and BPO vendors are all users.
5.	Are all 18 system boundaries in scope for PTaaS, or only a subset selected per testing cycle?	All system boundaries are in scope for formal annual test cycles and ad hoc testing at any time.
6.	Will USAC provide threat models or system classification (High/Moderate/Low) per boundary?	All boundaries are FIPS 199 Moderate at this time with no anticipation of any High, possibly one Low in the future.
7.	Will USAC provide cloud architecture diagrams (AWS, Azure, Oracle, Appian)?	Yes.
8.	What level of access will be granted for internal testing (domain user, privileged user, application admin)?	USAC can negotiate access as needed for the design of the test.
9.	How will remote internal testing access be provided (VPN, jump server, zero-trust proxy)?	USAC expects VPN to virtual machine to execute testing, but open to innovation.
10.	Of the ~220 applications, how many are in scope per cycle?	Cycles will be grouped by system, and most applications are within the systems.
11.	What technologies underpin the applications (Java, .NET, PHP, Node.js, Appian, etc.)?	USAC systems are deployed in multiple technologies with ongoing efforts to rationalize internal developed mission applications, leverage SaaS, and expand Appian for workflow/low-code.

Q#	Question	Answer
12.	Does USAC require full SAST/DAST/IaC testing, or only manual penetration testing?	We are interested in what is offered/recommended. USAC has Veracode SAST and DAST capabilities.
13.	Are cloud providers willing to grant authorization for pentests (AWS/Azure/Oracle/Appian)?	Yes.
14.	Which cloud services are in-scope (EC2, Lambda, API Gateway, SQL, Storage, Cognito/AAD, VPC)?	Those services supplying technology for USAC's mission systems. USAC uses AWS infrastructure along with premises infrastructure in a VPC, Appian, and M365/Azure for office automation and a customer service platform.
15.	Does USAC require cloud TTP-based testing (e.g., IAM privilege escalation, MFA bypass, session hijacking)?	We are interested in what is offered.
16.	What is the expected frequency for phishing, vishing, and pretext exercises?	Annual or bi-annual
17.	What is the scope for physical access testing at DC HQ (data centers, office floors, visitor areas)?	DC HQ with two floors in one building.
18.	Will badge cloning, tailgating, and lock bypass testing be permitted?	Yes.
19.	Does USAC require FISMA/NIST control mapping in reports?	Yes.
20.	What is the expected turnaround time for reports and retests?	We are interested in what is offered/recommended.
21.	What is the expected annual volume of tests across the 18 boundaries?	All system boundaries are in scope for formal annual test cycles and ad hoc testing at any time.
22.	Does USAC expect a 24×7 PTaaS SLA?	No, however, some testing may need to be performed during off-hours.
23.	What is the required annual cadence for a) External testing b) Internal network testing c) Application testing d) Cloud testing and e) Social engineering	All system boundaries are in scope for formal annual test cycles and ad hoc testing at any time. We are interested in what is offered for cadences. Social engineering cadence is at least annual.
24.	Testing Frequency & Consumption Model Can USAC provide an estimate as to how many full-scope penetration tests are anticipated per year across the ~18 FISMA boundaries?	All system boundaries are in scope for formal annual test cycles and ad hoc testing at any time.

Q#	Question	Answer
25.	Asset & Scope Size Of the ~18 FISMA system boundaries, how many external-facing web applications, unique external IP ranges, custom web apps/APIs, and separate cloud accounts (AWS, Azure, Appian Cloud, Oracle Cloud) would typically be in scope for a comprehensive test?	Most FISMA boundaries include web applications. This is an RFI, so that type of information would be provided in a potential RFP that may follow this RFI process.
26.	Social Engineering & Physical Testing What is the desired frequency and type of social engineering (e.g., email phishing only, or also vishing/SMiShing, and target population size), and does USAC require on-site physical/wireless testing at the Washington, DC headquarters?	All system boundaries are in scope for formal annual test cycles and ad hoc testing at any time. We are interested in what is offered for cadences. Social engineering cadence is at least annual. Physical/site testing would be one HQ site with wireless testing once annually.
27.	AI-Driven / Autonomous Testing Expectations The RFI references AI-enhanced social engineering, data-poisoning/AI attacks, and “identifying AI risk.” As of November 2025, no compliance-grade PTaaS solution exists that is fully autonomous (zero-human) across the entire scope described — all mature offerings are hybrid (AI/automation + certified human pen-testers for advanced TTPs, social engineering, and FISMA/NIST reporting). Is USAC open to a proven hybrid (AI enhanced + Human) model, or is fully AI-driven/no-human-in-the-loop testing a requirement?	We are interested in what is offered/recommended.
28.	Budget Target Is USAC able to provide an estimated budget annual target range for a comprehensive PTaaS program?	USAC does not have a budget range. This is an RFI, so that type of information would be provided in a potential RFP that may follow this RFI process.
29.	For the 220 applications/databases, how many are: • Internet-facing? • Internal-only? • Cloud-native vs. legacy/on-prem?	About 25% are accessible through internet, the rest are internal or supporting the external facing apps. About 60% are on cloud and we are progressively moving to cloud, including PaaS and SaaS solutions.

Q#	Question	Answer
30.	Are the mission systems containerized (Docker/K8s) or VM-based?	Very few systems are containerized now but will be in coming years.
31.	Are API endpoints part of the required test scope?	Some will be. We are interested in what is offered/recommended.
32.	For AWS testing, does USAC want: • IAM misconfiguration testing? • S3 bucket hardening validation? • Lambda/Serverless testing? • CloudTrail/CloudWatch logging validation?	We are interested in what is offered/recommended.
33.	For Appian Cloud, what level of penetration testing access is allowed by the vendor?	That is negotiable and we already do manual testing of the applications including penetration testing, with advance notice.
34.	Internal/External Network: Will USAC provide remote VPN access for internal network testing, or is on-site presence required? What is the scope of External Subnets. Will the offeror's Ip be whitelisted?	VPN. USAC can whitelist as required.
35.	Does internal testing include: • AD attack paths (Bloodhound-style)? • Kerberos abuse? • LAPS/credential harvesting?	We are interested in what is offered/recommended.
36.	Are EDR and SOC integrations expected for detection mapping (e.g., MITRE ATT&CK telemetry)?	We are interested in what is offered/recommended.
37.	How many SSIDs does USAC operate?	One
38.	Are WPA3, Radius/802.1X, or legacy PSK networks in use?	No
39.	Should phishing campaigns be: • One-time? • Quarterly? • Continuous (PTaaS automated)?	We are interested in what is offered/recommended.
40.	Is vishing allowed to target government-style hotlines, or internal numbers only?	We are interested in what is offered/recommended.

Q#	Question	Answer
41.	For physical access testing, does USAC require: • Badge cloning attempts? • Tailgating assessments? • Rogue device placement?	Potentially. We are interested in what is offered/recommended.
42.	What integrations does USAC require? • SIEM? (Splunk, Azure Sentinel) • Ticketing? (ServiceNow, Jira) • Vulnerability Scanners? (Qualys, Tenable)	Jira (Cloud) for ticketing. USAC uses Splunk for SIEM. Rapid7 for vulnerability.
43.	Does USAC require API access to findings for internal automation?	We are interested in what is offered/recommended.
44.	Does USAC want explicit testing against: • Prompt injection? • Data poisoning? • LLM API abuse? • Identity spoofing using AI-generated voice/phishing?	We are interested in what is offered/recommended.
45.	Should the PTaaS include adversary emulation mapped to MITRE ATT&CK?	Yes.
46.	For nominally invasive production testing, what level of acceptable disruption is allowed?	We are interested in what is recommended.
47.	Can USAC confirm whether all 18 FISMA system boundaries are expected to be in scope annually, or will testing be spread across a multi-year rotation?	See #23
48.	Does USAC expect PTaaS to fully replace all traditional manual penetration testing engagements, or will hybrid/manual components still be required for high-risk systems?	We are interested in what is recommended although PTaaS should replace all manual pen test engagements.
49.	Will USAC provide architectural diagrams/asset inventory during onboarding, or only during specific test cycles?	This is an RFI, so that type of information would be provided in a potential RFP that may follow this RFI process.

Q#	Question	Answer
50.	Does USAC anticipate a fixed testing cadence (e.g., quarterly), or does it require true on-demand "trigger-based" testing (e.g., KEV announcements, FedRAMP updates)?	See #23
51.	For social-engineering tests, does USAC want them scheduled regularly or triggered by specific events (e.g., new staff onboarding)?	Regularly.
52.	Which compliance requirements should PTaaS align to beyond FISMA and NIST 800-53? (e.g., FedRAMP, SOC 2, PCI, ISO 27001)	We are a FISMA shop because we administer Federal data on behalf of the FCC.
53.	Will USAC require deliverables to follow a specific reporting format required for FCC oversight?	Not applicable.
54.	Will USAC issue test accounts with elevated privileges to simulate insider threats, or only standard user accounts?	We are interested in what is offered/recommended.
55.	Will testing be restricted to specific maintenance windows for production-adjacent systems?	We are interested in what is offered/recommended, but generally, no.
56.	Does USAC want social engineering engagements to target: • All 1000–1500 internal users? • Specific departments only? • BPO vendors as well?	We are interested in what is offered/recommended. We have generally used a sampling approach in lieu of all users.
57.	For physical testing, will building access requirements (badges, escorts, NDAs) be provided?	As required.
58.	Does USAC expect PTaaS access to cloud consoles (AWS, Azure, Appian Cloud, Oracle Cloud), or only API-based / external testing?	We are interested in what is offered/recommended.
59.	For M365/Azure AD, is the testing expected to include Conditional Access, MFA bypass attempts, and OAuth app abuse scenarios?	We are interested in what is offered/recommended.
60.	What classification of data resides in the systems to be tested (e.g., PII, PHI, CUI), and are there restrictions on where PTaaS systems may store findings?	Most systems have some level of PII in production and sometimes in prod-like testing environments. All PII must be protected or redacted without any exfiltration.

Q#	Question	Answer
61.	How many stakeholder teams require separate reporting (IT Ops, Security, Compliance, Audit, Program Divisions)?	All reporting will be centralized to USAC Security.
62.	Are executive dashboards expected to integrate with USAC tools (e.g., Splunk, PowerBI, Jira, ServiceNow)?	We are interested in what is offered/recommended.
63.	Is FedRAMP authorization a requirement or a "nice to have"?	FedRAMP authorization is not anticipated for a PTaaS, however that could be a plus.
64.	Is USAC interested in Continuous Pen Testing (CPT) models?	We are interested in what is offered/recommended.
65.	Should the PTaaS include automated monthly scans or manual attack-based tests?	We are interested in what is offered/recommended.
66.	Does USAC require past performance in federal/state programs or commercials is also acceptable?	We prefer performance and familiarity with Federal requirements.
67.	Should pricing include optional add-ons (e.g., Purple Teaming, adversary simulation, AI Red Team)?	We are interested in what is offered/recommended.
68.	Is there an incumbent for this contract?	No.
69.	Are you willing to explore non-PTaaS providers with a path to becoming PTaaS in 2026?	No.
70.	Is your team open to a scoping call to get more details? If so, we are happy to accommodate your schedule, and we can disregard the rest of these questions	No.
71.	We understand you have about 220 applications/databases. Specifically, how many total applications would you like to have penetration tested for application security? Typically, custom/self-developed applications are tested for application security. Please clarify the 220 apps testing.	The applications are generally grouped into security boundaries with a number of enterprise applications that may not require Penetration Testing. The primary interest is our 18 FISMA authorized systems.

Q#	Question	Answer
72.	If there are multiple applications in the scope of application pentesting (not the internal/external pentest), please answer the following for each app: • What do the applications do? • How many different user roles are supported by the application? • What security-critical functions are provided by the applications (e.g. credit card transactions, money transfers, fraud detection, critical infrastructure, data accuracy, etc.)? • What are the application's architecture types (e.g. web, client/server, desktop, mobile, embedded, cloud, etc.)?	Please review the USAC.org website to understand the mission and programs of USAC.
73.	Regarding the network and infrastructure, how many in scope external IP addresses/range. URLs?	Not many external IP addresses because all users go through a centralized portal for MFA. There also are a few APIs that are accessible by external stakeholders.
74.	How many in scope internal IP addresses/range/URLs?	See #73
75.	How many external live hosts?	This is an RFI, so that type of information would be provided in a potential RFP that may follow this RFI process.
76.	How many internal live hosts?	This is an RFI, so that type of information would be provided in a potential RFP that may follow this RFI process.
77.	How many employees are considered in scope of social engineering/phishing attacks?	See #144
78.	What are the ideal start dates?	2nd Quarter CY2026 – This is an RFI, so that type of information would be provided in a potential RFP that may follow this RFI process.

Q#	Question	Answer
79.	Can you please provide more information about "stakeholder debriefings" in Section D: Overview of Potential Engagement? We ask because dependent on requirements, we need to factor this into our pricing.	We are interested in what is offered/recommended for how an offeror would communicate and discuss findings and issues.
80.	What is USAC's total number of publicly facing IPs? And/or is there an estimated number of publicly facing IPs)	See #73
81.	Is on-site physical access for testing the wireless network required? We can accommodate but this will impact cost.	We are interested in what is offered/recommended.
82.	Will all vendor participants receive the full list of questions asked by every RFI participant?	Yes.
83.	For the 220 applications/databases, how many are: • Internet-facing? • Internal-only? • Cloud-native vs. legacy/on-prem?	See #29.
84.	Are the mission systems containerized (Docker/K8s) or VM-based?	Most are not; we are progressively moving into containerization for internal developed systems (not PaaS or SaaS).
85.	Are API endpoints part of the required test scope?	Likely, yes.
86.	For AWS testing, does USAC want: • IAM misconfiguration testing? • S3 bucket hardening validation? • Lambda/Serverless testing? • CloudTrail/CloudWatch logging validation?	We are interested in what is offered/recommended. In general, yes.
87.	For Appian Cloud, what level of penetration testing access is allowed by the vendor?	Dynamic testing at application level.
88.	Will USAC provide remote VPN access for internal network testing, or is on-site presence required? What is the scope of External Subnets. Will the offeror's Ip be whitelisted?	This is an RFI, so that type of information would be provided in a potential RFP that may follow this RFI process. We anticipate VPN access and network access will be supported as needed.

Q#	Question	Answer
89.	Does internal testing include: • AD attack paths (Bloodhound-style)? • Kerberos abuse? • LAPS/credential harvesting?	We are interested in what is offered/recommended.
90.	Are EDR and SOC integrations expected for detection mapping (e.g., MITRE ATT&CK telemetry)?	In general, yes. We are interested in what is offered/recommended.
91.	How many SSIDs does USAC operate?	Two.
92.	Are WPA3, Radius/802.1X, or legacy PSK networks in use?	No.
93.	Should phishing campaigns be: • One-time? • Quarterly? • Continuous (PTaaS automated)?	See #16 and #26.
94.	Is vishing allowed to target government-style hotlines, or internal numbers only?	This is an RFI, so that type of information would be provided in a potential RFP that may follow this RFI process. We are interested in what is offered/recommended.
95.	For physical access testing, does USAC require: • Badge cloning attempts? • Tailgating assessments? • Rogue device placement?	In general, yes. We are interested in what is offered/recommended.
96.	What integrations does USAC require? • SIEM? (Splunk, Azure Sentinel) • Ticketing? (ServiceNow, Jira) • Vulnerability Scanners? (Qualys, Tenable)	We use Splunk, Jira, and Rapid7 InsightVM. Jira integration would be very helpful. We are interested in what is offered/recommended.
97.	Does USAC require API access to findings for internal automation?	We are interested in what is offered/recommended.

Q#	Question	Answer
98.	Does USAC want explicit testing against: • Prompt injection? • Data poisoning? • LLM API abuse? • Identity spoofing using AI-generated voice/phishing?	In general, yes. We are interested in what is offered/recommended.
99.	Should the PTaaS include adversary emulation mapped to MITRE ATT&CK?	In general, yes. We are interested in what is offered/recommended.
100.	For nominally invasive production testing, what level of acceptable disruption is allowed?	Minimal if any.
101.	Can USAC confirm whether all 18 FISMA system boundaries are expected to be in scope annually, or will testing be spread across a multi-year rotation?	See #23.
102.	Does USAC expect PTaaS to fully replace all traditional manual penetration testing engagements, or will hybrid/manual components still be required for high-risk systems?	See #48.
103.	Will USAC provide architectural diagrams/asset inventory during onboarding, or only during specific test cycles?	See #49.
104.	Does USAC anticipate a fixed testing cadence (e.g., quarterly), or does it require true on-demand “trigger-based” testing (e.g., KEV announcements, FedRAMP updates)?	See #50.
105.	For social-engineering tests, does USAC want them scheduled regularly or triggered by specific events (e.g., new staff onboarding)?	See #51.
106.	Which compliance requirements should PTaaS align to beyond FISMA and NIST 800-53? (e.g., FedRAMP, SOC 2, PCI, ISO 27001)	See #52.
107.	Will USAC require deliverables to follow a specific reporting format required for FCC oversight?	See #53.

Q#	Question	Answer
108.	Will USAC issue test accounts with elevated privileges to simulate insider threats, or only standard user accounts?	See #54.
109.	Will testing be restricted to specific maintenance windows for production-adjacent systems?	See #55.
110.	Does USAC want social engineering engagements to target: • All 1000–1500 internal users? • Specific departments only? • BPO vendors as well?	See #56
111.	For physical testing, will building access requirements (badges, escorts, NDAs) be provided?	See #57.
112.	Does USAC expect PTaaS access to cloud consoles (AWS, Azure, Appian Cloud, Oracle Cloud), or only API-based / external testing?	See #58.
113.	For M365/Azure AD, is the testing expected to include Conditional Access, MFA bypass attempts, and OAuth app abuse scenarios?	See #59.
114.	What classification of data resides in the systems to be tested (e.g., PII, PHI, CUI), and are there restrictions on where PTaaS systems may store findings?	See #60
115.	How many stakeholder teams require separate reporting (IT Ops, Security, Compliance, Audit, Program Divisions)?	See #61
116.	Are executive dashboards expected to integrate with USAC tools (e.g., Splunk, PowerBI, Jira, ServiceNow)?	See #62
117.	Is FedRAMP authorization a requirement or a “nice to have”?	See #63
118.	Is USAC interested in Continuous Pen Testing (CPT) models?	See #64
119.	Should the PTaaS include automated monthly scans or manual attack-based tests?	See #65

Q#	Question	Answer
120.	Does USAC require past performance in federal/state programs or commercials is also acceptable?	See #66
121.	Should pricing include optional add-ons (e.g., Purple Teaming, adversary simulation, AI Red Team)?	See #67
122.	Is FedRAMP authorization a requirement or a "nice to have"?	See #63
123.	Does the ~18 FISMA authorized system boundaries incapsulate the entire testing scope?	90% of the scope.
124.	Provide the number of External IPs (incl. firewall, VPNs, etc.)	See #73
125.	Please share the number of Internal servers, and domain controllers	This is an RFI, so that type of information would be provided in a potential RFP that may follow this RFI process.
126.	Please provide an approximate number of network segments (VLANs).	4 but will be more in the future with improved segmentation.
127.	Please provide the number of sites/locations to be tested (if more than one).	One HQ office.
128.	Are the IPs allocated dynamically or statically?	Primarily dynamic, however, this is an RFI, so that type of information would be provided in a potential RFP that may follow this RFI process.
129.	How will access to the internal network be provided (e.g., VPN, OVA, AMI, etc.)? • Vendor can provide OVA and/or AMI files for internal foothold.	See #88.
130.	Please provide an approximate number of web applications accessible: • External web applications • Internal web applications	Most of the 18 security boundaries have multiple external and internal web apps.
131.	Please provide an approximate number of dynamic pages in each web application.	This is an RFI, so that type of information would be provided in a potential RFP that may follow this RFI process.

Q#	Question	Answer
132.	Please provide the average number of user roles required for testing.	This is an RFI, so that type of information would be provided in a potential RFP that may follow this RFI process.
133.	Are these applications tested with or without authentication?	We are interested in what is offered/recommended.
134.	Please provide an approximate number of mobile applications to be tested.	None.
135.	Does the mobile application testing include both iOS and Android platforms?	Not applicable.
136.	Are these mobile applications tested with or without authentication?	Not applicable.
137.	Please provide the number of screens in each mobile application.	Not applicable.
138.	Please provide the number of user profiles within the mobile application.	Not applicable.
139.	Please confirm if social engineering attacks are to be performed on 1000 to 1500 users or is it just a subset of those users?.	See #56
140.	Please provide an approximate number of phishing campaigns to be sent per user.	See #56
141.	Please provide the Cloud service provider	USAC uses AWS for cloud infrastructure, M365/Azure for some systems and internal office automation/support.
142.	Number of Cloud accounts for assessment	This is an RFI, so that type of information would be provided in a potential RFP that may follow this RFI process.
143.	Are there any restrictions or guidelines regarding testing methods, such as limitations on the use of invasive techniques, requirements for testing in production versus staging environments, or other considerations related to the safety, scope, or timing of penetration testing activities?	We are interested in what is offered/recommended.

Q#	Question	Answer
144.	What is the expected scope and depth of social engineering testing? Will it focus solely on phishing, or also include physical access attempts and pretext calling? Should testing be conducted for all 200,000 users, or targeted toward high-risk groups such as IT staff with elevated privileges and executives?	Social engineering is focused on internal staff and BPO vendor users. We are interested in what is offered/recommended. See #56
145.	Can you clarify which systems, applications, or user groups are considered highest priority for initial penetration testing, and whether there are any specific compliance or operational deadlines driving this prioritization?	This is an RFI, so that type of information would be provided in a potential RFP that may follow this RFI process..
146.	What existing security tools, SIEMs, or reporting platforms does USAC currently use, and are there preferred formats or integration requirements for penetration testing results and dashboards?	See #96
147.	Is USAC interested in ongoing, continuous penetration testing and threat monitoring, or is the focus primarily on scheduled, point-in-time assessments? How should findings that require urgent remediation be communicated and escalated?	We are interested in what is offered/recommended. In general, any significant (Critical/High) finding should always be reported immediately so that remediation can be done followed by a retest.
148.	Are there particular concerns or requirements around social engineering, AI-enhanced phishing, or adversarial AI threats that you would like the PTaaS solution to address in greater depth?	We are interested in what is offered/recommended.
149.	For physical access and wireless network testing at USAC headquarters, are there specific scenarios, controls, or compliance standards you want to see addressed?	We are interested in what is offered/recommended.
150.	Can you provide previous penetration test results to identify gaps, misses and know issues and successes?	USAC will provide intelligence to help prioritize when onboarding a vendor for PTaaS.

Q#	Question	Answer
151.	Are there any systems or environments excluded from the PTaaS engagement (e.g., legacy systems, certain cloud services)?	Yes – we have some deprecated legacy systems being replaced or in process of decommissioning.
152.	Could you clarify whether physical access testing at the DC headquarters is required, and if so, what objectives or considerations are guiding this requirement?	We are interested in what is offered/recommended. USAC has one main building in DC with two SSIDs.
153.	Will USAC provide dedicated test environments that mirror production, or will testing occur in production systems?	We are interested in what is offered/recommended. Generally, we have tested production-like test environments.
154.	For AWS, Azure, and Oracle Cloud environments, are there specific compliance or segmentation requirements for testing?	This is an RFI, so that type of information would be provided in a potential RFP that may follow this RFI process.
155.	Does USAC require integration with existing vulnerability management or SIEM tools?	See #96
156.	Can USAC elaborate on expectations for identifying AI-related risks (e.g., adversarial attacks, data poisoning)?	We are interested in what is offered/recommended.
157.	Is FedRAMP authorization required for the PTaaS provider, or is alignment with FISMA/NIST sufficient?	See #63
158.	Are reports expected to follow specific templates or standards beyond Common Vulnerability Scoring System (CVSS) scoring (e.g., NIST SP 800-115 format)?	We are interested in what is offered/recommended. In general, CVSS is essential.
159.	What are USAC's requirements for data residency and confidentiality during testing and reporting?	We are interested in what is offered/recommended. See
160.	Will USAC provide a formal Rules of Engagement document, or should the vendor propose one?	We are interested in what is offered/recommended.
161.	How quickly must the PTaaS provider respond to ad-hoc or emergent threat-based testing requests?	We are interested in what is offered/recommended.
162.	Is retesting of remediated vulnerabilities included in scope, and how soon after remediation should it occur?	Yes, retesting is in scope and timing is opportunistic.
163.	Does USAC prefer subscription-based pricing, pay-per-test, or hybrid models?	We are interested in what is offered/recommended.

Q#	Question	Answer
164.	Are there any budgetary ceilings or cost parameters USAC can share for planning purposes?	See #28
165.	Will USAC require live demos for shortlisted vendors, and if so, what specific capabilities should be showcased?	No demos are required for the RFI at this time, but USAC can determine the need later.
166.	Is USAC open to managed services beyond PTaaS (e.g., vulnerability management, threat intelligence)?	No.
167.	Could the USAC please confirm whether this is a new initiative or an existing engagement?	PTaaS is new; Penetration Testing has been performed consistently for at least 5 years.
168.	Could the USAC provide an estimated budget or a Not-to-Exceed (NTE) amount for this contract?	See #28 This is an RFI, so that type of information would be provided in a potential RFP that may follow this RFI process.
169.	Could the USAC please provide the anticipated project timeline, including key milestones and the overall expected duration of the engagement?	See # 168 This is an RFI, so that type of information would be provided in a potential RFP that may follow this RFI process.
170.	Could the USAC please clarify whether it intends to award this RFP to a single vendor or multiple vendors? If multiple awards are anticipated, could the USAC specify the expected number of vendors to be selected?	See # 168 This is an RFI, so that type of information would be provided in a potential RFP that may follow this RFI process.
171.	Can USAC provide the approximate number of public IP ranges and total public IP addresses expected to be in scope?	See #73.
172.	How many internal subnets, VLANs, and total internal IPs are expected to be included in internal penetration testing?	One VLAN. See #73, #88.
173.	Of the ~220 applications/databases, how many does USAC expect to include in testing each year?	See #10, #29.
174.	For the 18 FISMA system boundaries, how many boundaries does USAC expect to assess annually?	See #5

Q#	Question	Answer
175.	For 800–1200 laptops: • Should all endpoints be tested? What's the exact count? • Or only sample-based testing? (If sample-based, what sample size?)	We are interested in what is offered/recommended. In general, we anticipate sampling at a statistically valid count.
176.	Wireless Testing Scope at HQ • How many access points? • How many floors / physical zones? • Any guest vs internal separation?	See #26
177.	How many users will be targeted in phishing tests? • Internal users (1000–1500)? • Contractors/BPOs? • External users (~200,000) – included or excluded?	See #56
178.	How often does USAC expect phishing tests to run? • Quarterly? • Monthly? • On-demand?	See #16.
179.	Types of Social Engineering; Please confirm required methods: • Email phishing? • SMS phishing (smishing)? • Voice phishing (vishing)? • Pretext phone calls? • Physical tailgating tests?	We are interested in what is offered/recommended.
180.	How many attempts are expected for physical access testing? (e.g., 1 attempt, 3 attempts, multiple scenarios)	This is an RFI, so that type of information would be provided in a potential RFP that may follow this RFI process. We are interested in what is offered/recommended.

Q#	Question	Answer
181.	How many individual pentests does USAC anticipate requesting per year?	This is an RFI, so that type of information would be provided in a potential RFP that may follow this RFI process. We are interested in what is offered/recommended.
182.	What is USAC's expectation for turnaround time for ad-hoc tests triggered by: • Active threats • KEV alerts • Zero-day vulnerabilities	We are interested in what is offered/recommended. However, the urgency of threat/risk will determine expectations.
183.	When USAC refers to "continuous testing," do they mean: • Automated attack surface monitoring, or • The ability to launch tests at any time, or • Both?	Automated attack surface monitoring, primarily. We are interested in what is offered/recommended.
184.	What is the expected SLA for notifying USAC of critical/high vulnerabilities detected during testing? (Immediate, 4 hours, 24 hours?)	One business day as a maximum.
185.	Does USAC expect the vendor to map findings to: • NIST 800-53 controls? • NIST 800-115 testing methodology? • Both?	Both.
186.	Is USAC able to share a planning budget range for this program to help align pricing models?	See #28
187.	Can USAC clarify the anticipated contract duration when the formal RFP is released? (For example: 1 year, 2 years, 3 years, or multi-year?)	Multi-year, potentially 3-5 years

Q#	Question	Answer
188.	Can USAC please clarify whether the intent of this RFI is to obtain only a Penetration Testing as a Service (PTaaS) technology platform, only professional penetration testing services, or a combination of both the platform and human-led testing services? This will help us provide more accurate scope and pricing information.	Primarily a PTaaS platform replacing manual-only engagements. We are interested in what is offered/recommended where human-led testing is superior.
189.	Can USAC clarify what types of AI-related attacks they are specifically concerned about (e.g., deepfake phishing, adversarial ML, data poisoning)?	We are interested in what is offered/recommended. AI is emerging and change, so we are interested in services responsive to emerging threats.
190.	Can USAC clarify whether the PTaaS solution is expected to operate in an agent-based, agentless, or hybrid model?	We are interested in what is offered/recommended.
191.	Are there any E-Rate eligibility, certifications, or compliance obligations that vendors must meet in order to participate in the PTaaS procurement?	Not applicable.
192.	With the week of 11/24 being a holiday week, would USAC consider extending the due date a week to give offerors enough time to respond?	RFI Due date is extended to December 15, 2025, 11:00 AM ET.
193.	Are there any parts of USAC's program they would want excluded from testing?	This is an RFI, so that type of information would be provided in a potential RFP that may follow this RFI process.
194.	The RFI submission instructions indicate that the subject line of the submission should be "Response to RFI XXX-24-188 – Penetration Testing as a Service", can USAC confirm if this should be "Response to RFI IT-25-188 – Penetration Testing as a Service" instead?	Response to RFI IT-25-188 -- PTaaS
195.	Approximately how many endpoints/IPs should offerors expect for external testing?	See #73.
196.	Can USAC provide an estimated period of performance to allow offerors to provide a more accurate pricing estimate?	See #187.
197.	Can USAC confirm if the cover page and table of contents count toward page limit requirements?	Cover page and table of content is excluded from the page count.

Q#	Question	Answer
198.	Is there an existing contract where a vendor is performing penetration testing?	See #167.
199.	Does USAC anticipate requiring an "independent" PTaaS provider (i.e., not previously involved in system development, assessment, or operations)? If so, how will independence be defined?	No.
200.	Can USAC describe its current penetration testing posture, tools, and testing cadence to help vendors determine the right-fit solution?	See other Q&A.
201.	Can USAC clarify the scope of systems expected to be covered by the PTaaS solution (public-facing applications, internal systems, cloud infrastructure, APIs, mobile apps, etc.)?	USAC does not develop or deploy mobile apps. Public and internal systems are of primary interest and that would encompass VPC, cloud infrastructure, APIs, PaaS, etc.
202.	Does USAC intend for PTaaS to support continuous automated testing, periodic manual testing, or a hybrid approach?	We are interested in what is offered/recommended.
203.	Does USAC prefer proprietary platforms, COTS tools, open-source frameworks, or a combination for the PTaaS environment?	We are interested in what is offered/recommended.
204.	What level of automated reporting and dashboarding does USAC anticipate (e.g., real-time dashboards, executive summaries, FISMA/NIST mapping)?	We are interested in what is offered/recommended.
205.	Does USAC expect the PTaaS platform to integrate with existing vulnerability management or ticketing systems (e.g., Jira, ServiceNow, Tenable, Qualys)?	See #96, #42.
206.	Which cloud platforms and environments (AWS, Azure, GCP, SaaS systems) must be included within scope?	See #141, #58
207.	Is USAC seeking PTaaS capabilities that include red teaming, purple teaming, social engineering, or adversary simulation exercises?	USAC is interested in red/purple teaming as an option, social engineering test is required, adversary simulation as an option.

Q#	Question	Answer
208.	Does USAC have a target budget range or ceiling for the anticipated PTaaS contract to help vendors scale their solutions appropriately?	See #28
209.	Can USAC share historical level-of-effort (LOE) data or number of annual penetration tests previously performed to help estimate staffing and resource needs?	See #21, #23, #26
210.	Is USAC seeking subscription-based PTaaS pricing, per-engagement pricing, or a hybrid model?	We are interested in what is offered/recommended.
211.	Are there known challenges or limitations with USAC's current penetration-testing approach that the PTaaS model is intended to address?	Availability, ability to perform multiple penetration tests concurrently (on different systems), ability to retest once remediated ad hoc any time, responsiveness to emerging threat vectors.
212.	Does USAC expect the PTaaS provider to support knowledge transfer, training, or staff augmentation as part of the engagement?	We are interested in what is offered/recommended. However, in general we expect reporting to be informative and provide references (like OWASP or NIST) to support remediation.
213.	Can USAC provide approximate system counts, IP ranges, number of applications, or user population to support accurate pricing estimates?	Several answers to questions cumulatively answer this question.
214.	Can you please provide more information about "stakeholder debriefings" in Section D: Overview of Potential Engagement? We ask because dependent on requirements, we need to factor this into our pricing.	See #79
215.	What is USAC's total number of publicly facing IPs? And/or is there an estimated number of publicly facing IPs?	See #73
216.	Is on-site physical access for testing the wireless network required? We can accommodate but this will impact cost.	See #26, #41
217.	What are the considerations for determining whether testing onsite of particular systems will be required or preferred?	All systems except physical environment and wireless can be tested remotely. See #26.

Q#	Question	Answer
218.	What is the anticipated time frame that USAC expects all of these systems to be tested within? Are there any anticipated blackout dates for testing?	See #5. There will be blackout dates depending on business cycles, development planning, and environment
219.	How many personnel will USAC involve to ensure testers will have access to systems? We anticipate that many of these systems can be tested in parallel.	See #8 and TBD depending on the planning. We are interested in what is offered/recommended.
220.	What is the intended total length of this contract for PTaaS?	See #187 and #168
221.	Mobile App Testing is listed in-scope but later it's mentioned that USAC does not develop them. It is unclear if we are able to test these if they are third-party mobile applications. Please confirm if any mobile apps are in scope and if they are developed by USAC.	See #201.
222.	Our quoting process requires a scoping call, or for larger quantities, complete our scoping questionnaire. In order to provide accurate pricing, can you complete our scoping questionnaire?	See #168 – This is an RFI, so that type of information would be provided in a potential RFP that may follow this RFI process.
223.	Is a US-based, foreign-owned entity acceptable?	Yes, as long as the company is based in US and operates from within the US.
224.	Is it possible to leverage non-US resources in non-sanctioned territories and/or non-US Citizens to deliver these services?	No, all work must be performed from within the US and all resources must be in the US.
225.	Are there limitations to the use of AI to deliver these services?	Negotiable and in alignment with USAC's AI policy.
226.	What are the core decision making criteria for these services?	To avoid automatic rejections, response should at least adhere to the followings: 1. RFI submission instructions. 2. Providing responses to technical scope of work.
227.	Is it acceptable that network testing, application testing, IAM assessments and social engineering are separate service lines?	Negotiable. We are interested in what is offered/recommended.
228.	What is the frequency of social engineering engagements and number of users for consideration in each attempt?	See #16, #26, #144

Q#	Question	Answer
229.	Does USAC leverage a phishing platform today? If yes, how many licenses are included? Is this type of service in-scope?	Phishing test is in-scope. No platform today.
230.	How many active external IPs are there?	See #73
231.	How many internal IPs / total devices are in scope?	This is an RFI, so that type of information would be provided in a potential RFP that may follow this RFI process.
232.	Is the goal for the application testing to also be done in a “continuous” manner incorporating delta testing where we are part of your agile dev teams, or are these more periodic, like monthly or quarterly?	We are interested in what is offered/recommended. However, the initial interest is replacing our annual manual pen tests.
233.	How many of the 220 applications would require OWASP LLM Top 10 testing?	
234.	How many of the 220 applications are mobile applications?	None.
235.	Is Android and iOS testing required for the mobile applications?	Not applicable.
236.	How many of the applications are externally facing?	See #29
237.	Are dynamic application scanning tool results available today for all of the applications? If yes, what tool?	Not yet, we are beginning to use Veracode DAST
238.	Are there other locations beyond the Washington, DC headquarters that may require wifi / physical security testing?	No.
239.	What is the frequency of the on-site testing?	Annual.
240.	What type of Identity Access Management (IAM) “testing” is expected for this project?	We are interested in what is offered/recommended.
241.	What IAM tools are currently being used?	Okta
242.	What type of production system monitoring is USAC looking for? Is there a SIEM in place today? Is it managed and monitored internally or is that outsourced?	See #3, #42
243.	Is a third-party platform in place for the current program? If yes, is that managed in house or from the platform provider?	No third-party platform is in place for PTaaS.

Q#	Question	Answer
244.	Would triaging and/or validating Vulnerability Disclosure Program submissions be in scope for this engagement?	We are interested in what is offered/recommended. That may be helpful.
245.	Is internal ticket management from this platform something USAC would be interested in?	USAC is invested in Jira for internal ticketing.