2026 Penetration Testing Services RFP FAQ

1. General Scoping

   a) Will this be Grey Box (credentials provided) or Black Box (no access)?
   Application credentials will be provided.
   b) What level of access will be provided for credentialed web application testing (e.g., standard user, administrator, multiple roles)?
   Multiple roles depending on the application.
   c) Will testing occur on production or test/dev environments?
   Both, production for the network testing and UAT for internal apps.
   d) Any compliance drivers (SOC 2, HIPAA, PCI, etc.)?
   No
   e) To confirm, all 5 types of tests are to be conducted in each of the four rounds of testing?
   Negative, the Physical Assessment and WiFi assessment will only need to be conducted once over the 2-year contract.
   f) What is the allocated budget for this particular contract?
   No specified budget
   g) Who is the current incumbent and what are they charging for these services?
   You need to submit a Public Records request through our Legal department.
   h) What security controls are present at the physical location (e.g., badge access, security guards, cameras, locked server rooms)?
   This should be discovered by the testers during the recon phase.
   i) What are the minimum insurance requirements for this engagement (e.g., Cyber Liability, Errors & Omissions, General Liability limits)?
   $2million in coverage

2. External Network Pentest (ENPT)

   a) Are all 300 IPs internet-facing, or does this include internal ranges?
   All public facing
   b) Will credentials be provided for VPN/remote access portals?
   If required yes
   c) Any specific services to focus on (VPN gateways, mail servers, CDN)?
   No
   d) Any critical/legacy systems to avoid?
   No

3. Web Application Pentest (WAPT)

a) How many unique pages/workflows per application (approximate)?
Approximately 20
b) How many user roles per application (guest, user, admin)?
Approximately 3
c) Do the applications have backend APIs in scope?
Yes
d) Are the applications cloud-hosted or on-prem?
Cloud-hosted
e) Will architecture docs/API specs be provided?
No
f) Any MFA, SSO, or complex login flows?
MFA for any system access.
g) Any sensitive integrations (payments, PII/PHI)?
PII

4. Wireless Assessment

a) How many SSIDs are in scope at the physical location?
Approximately 7
b) Approximate size of site (floors, buildings)?
2 connected buildings, one building has 4 floors one building has 6 floors.
c) Authentication type (WPA2, WPA3, 802.1X/Enterprise)?
WPA2 Enterprise
d) Will enterprise credentials be provided for testing?
No for Wifi testing
e) Any restrictions on testing methods (no deauth attacks, etc.)?
No

5. Physical Pentest

a) What activities are in scope (building entry, tailgating, badge cloning, device drops)?
No restrictions on entry tactics
b) Approximate facility size (single building, multi-floor)?
2 connected buildings, one building has 4 floors one building has 6 floors.
c) Are social engineering tactics allowed on-site?
Yes
d) What hours are permitted for testing (business hours, after hours)?
No restrictions

e) Are there any areas within the building that are designated as off-limits during physical testing?
Yes

f) What security controls are present at the physical location (e.g., badge access, security guards, cameras, locked server rooms)?
This should be discovered by the testers during the recon phase.

6. Social Engineering/Phishing

a) How many employees will be targeted?
Approximately 50

b) What vectors are in scope (email phishing, vishing/phone calls, SMS)?
Email Phishing and Vishing, no SMS

c) Will RIHousing provide a target list with emails/phone numbers?
Yes

d) Should a credential-capture site be used?
No

e) Any themes/lures off-limits?
No adult themes or explicit material