CTPF

Chicago Teachers’ Pension Fund

Questions and Answers #1 Related to the RFP for EXTERNAL AND INTERNAL PENETRATION TESTING SERVICES

**1.** How many internal IP’s are in scope?

Answer: 7880.

**2.** How many external IP’s are in scope?

Answer: 265.

**3.** Clarify what they want included when conducting a Firewall Assessment? Is that a pen test of the firewall or a configuration assessment?

Answer: Both.

**4.** Will a physical site security review be necessary? If so please complete our wireless scoping questionnaire for this portion of the test.

Answer: Yes.

**5.** Is there only one website? ctpf.com

Answer: ctpf.org is our public facing website. There are an additional two internet facing web applications (member portal, employer portal) that are in scope. One internal web-based application (pension administration system) will also be included in scope.

**6.** How many user roles will need to be tested for that website?

Answer: ctpf.org does not have user authentication. Our member portal web application has a single role for testing. Our employer portal web application has 3 roles (admin, user, read only) to be tested. Our internal pension application has 2 roles (admin, user) that will require testing.

**7.** If there are more than one website in scope? What are the URl’s and how many user roles will be in scope?

Answer: Please refer to Answer Nos. 5 and 6.

**8.** For the wireless testing, how many locations and how many SSIDs are in scope?

Answer: 2

**9.** For the physical social engineering project, how many locations?
Answer: 1

**10.** Will project base pricing be sufficient instead of hourly?
Answer: A quote for an hourly rate is required.

**11.** What is the timeline for testing?
Answer: This RFP will cover multiple projects during each fiscal year. The timing of testing will be agreed upon between CTPF and the selected vendor.

**12.** How many locations for WiFi penetration testing are in scope and how far apart is each location?
Answer: 2 separated by a floor.

**13.** How many SSID's are in scope for WiFi penetration testing?
Answer: 2

**14.** How many staff do you want socially engineered with phishing attacks?
Answer: Sampling methodology can be used to select the number of staff.

**15.** How many locations and why types of locations do you want tested for physical access security
Answer: 1 corporate office location

**16.** What assets need to be assessed as part of scope for the External Network Penetration testing (e.g., routers, switches, firewalls, servers, etc.)?
Answer: Routers, switches, firewalls, and servers and systems are in scope assets.

**17.** What is the total number of IP addresses to be factored in for Network Penetration testing?
Answer: Refer to Answers Nos. 1 and 2.

**18.** What is the total number of firewalls to be factored as part of the Firewall assessment scope?
Answer: Refer to Answers Nos. 3 and 16.

**19.** "Is the assessment scope limited only to Firewall Configurations assessment or should it include a Rule based Assessment as well? If a Rule based assessment is in-scope will CTPF provide the testers with a firewall rules dump?"
Answer: Rules-based analysis is in scope.

**20.** Please define the frequency of External Network Penetration testing scope (e.g., Once, Monthly, Quarterly, Bi-annually, Annually)?

Answer: Annually with re-testing iterations for proof of effective remediation.

**21.** How many network devices are to be factored in for Internal Network Penetration testing scope (e.g., routers, switches, firewalls)?

Answer: 14 switches, 2 firewall appliances (FTD), 1 firewall management appliance (FMC), 2 routers, 14 access points, 2 wireless controllers, 2 FI switches.

**22.** "Are servers and workstations also part of the Internal Network Penetration testing scope? If yes, please specify the number for servers and workstations separately. “

Answer: Yes, approximately 180 servers and 250 workstations.

**23.** Can the Internal Network Penetration testing be carried out remotely?

Answer: We are open to proposals detailing how the internal network penetration testing can be carried out remotely.

**24.** Please define the frequency of Internal Network Penetration testing scope, e.g. once, Monthly, Quarterly, Bi-annually, Annually, etc.

Answer: Please refer to Answer No. 20 above.

**25.** How many websites and web applications are to be factored for the Website Penetration testing scope?

Answer: Please refer to Answers Nos. 5 and 6

**26.** "Please specify the sizing of all the in-scope websites and applications in terms of the number of dynamic pages, refer to the below-mentioned sizing criteria: Small (up to 50 web pages) Medium (up to 100 web pages) Large (up to 150 web pages) Extra Large (up to 200 web pages)."

Answer: ctpf.org website would be Medium. Two internet web applications would be Small. Internal web application would be Large.

**27.** What type of testing is desired as part of the Web Application testing scope (e.g. BlackBox testing, GrayBox testing, or both)?

Answer: Both types

**28.** "Are there any APIs or web services associated with the in-scope applications? If yes, please specify the number of API or web services for each application separately."

Answer:

Employer Portal to Internal Pension Application – 20 API endpoints

Member Portal to Internal Pension Application – 17 API endpoints
Internal pension application to external party – 4 API endpoints.

**29.** Are any of the in-scope websites and applications only exposed internally? If yes, please specify the number of such applications, including sizing.

Answer: Please refer to Answers Nos. 5 and 26.

**30.** Please define the frequency of the Website Penetration testing scope (e.g., Once, Monthly, Quarterly, Bi-annually, Annually).

Answer: Annually or when a website application update occurs.

**31.** Is there a dedicated test environment available for conducting the testing?

Answer: There is only an application development sandbox environment.

**32.** How many access points (APs) are to be factored for the wireless Penetration Testing scope?

Answer: 19

**33.** How many office locations are in scope for wireless Penetration Testing?

Answer: One office, and located on two floors.

**34.** What specific types of social engineering techniques do you want to assess (e.g., phishing, spear phishing, vishing, smishing, pretexting, tailgating)?

Answer: All listed types.

**35.** Are there any specific departments, teams, or individuals that should be targeted?

Answer: As appropriate.

**36.** Please specify the number of intended victims to be targeted.

Answer: Refer to Answer No.14.

**37.** Are there any specific social engineering scenarios to be tested?

Answer: Social engineering scenarios that are not highly challenging will not accomplish objectives. The social engineering scenarios need to be highly credible and well executed to be effective.

**38.** Are there any compliance requirements (e.g., PCI DSS, HIPAA) to consider?

Answer: HIPAA.

**39.** Are there any specific testing methodologies or frameworks that need to be followed for Network and Application Penetration testing?

Answer: The proposal should reference which PTF (Pen Testing Framework) or PTF's will be followed for the testing.

**40.** What will be the frequency of the ad-hoc penetration requests? Please share the approximate number or requests.

Answer: Ad-hoc penetration testing will be requested for any major release of a CTPF's two external web applications. The frequency will be 1-2 releases per application per year.

**41.** Will Static Application Security Testing (SAST) be part of the scope of work?

Answer: No.

**42.** Please specify the number of rounds of confirmation / validation testing that needs to be factored in as part of the assessment scope?

Answer: 3.

**43.** Is CTPF open to exploring non-USA/Canada based hybrid options to provide the requested services and solutions? Our clients typically want to leverage this option to get access to our global pool of cybersecurity analysts/testers in a cost-efficient manner. Please confirm.

Answer: Yes.

**44.** Can CTPF provide any information on the budget required to support these services? (e.g., allocated budget details).

Answer: CTPF does not release budget information.

**45.** Is CTPF currently using any service providers that are assisting in performing the requested services? If so, who are these providers?

Answer: Yes. Crowe, LLP.

**46.** Is there an incumbent who has performed the in-scope testing in the past?

Answer: Yes. Crowe, LLP.

**47.** How many actual Internal devices are in Scope?

Answer: Approximately 40 .

**48.** How many actual External devices are in Scope?

Answer:  0.

**49.** How many External and/or Internal websites are in scope?

Answer: Refer to Answer No. 5.

**50.** How many external IPs/Subnets will be in scope?

Answer:  Refer to Answer No. 2

**51.** How many internal IP/Subnets will be in scope?

Answer: Refer to Answers Nos. 1, 2 and 52.

**52.** External Network Penetration Testing

a. How many "live" (answers on at least one port) systems (IPs/hostnames) in total are in scope for testing?

Answer available upon signing a Non-Disclosure Agreement (NDA).

b. What are the IP network ranges in scope for testing?

Answer available upon signing NDA.

c. What external domain names (company.com, companyproduct.com, etc.) are in scope for testing?  All DNS records in scope should be included in the total live systems count.

i. ctpf.org
ii. ctpfers.org
ii. myctpf.org

Answer: See Answers above.

**53.** Internal Network Penetration Testing

a) Can testing occur from a single, central location and network port?
b) If not, please how many physical locations and ports should testing occur from?
c) How many Active Directory Forest and domains exist?
d) If multiple, please describe their trusts.
e) How many "live" (answers on at least one port) systems (IPs/hostnames) in total are in scope for testing?

Answer:

a. Yes
b. N/A
c. 1
d. N/A
e. Answer available upon signing NDA.

**54.** CTPF Websites Penetration Testing

a. How many web applications are in scope for testing?
b. Please describe the user roles to be tested. (Administrator, Manager, User, etc.)
c. How many unique pages or screens does each web application support?
d. Is a test, QA (Quality Assurance), UAT (User Acceptance Testing), staging, or otherwise non-production environment available for testing?

Answer: Please refer to previous Answers:

a. See 5

b. See 6

c. See 26

d. Yes

**55.** Wireless Security Scanning

How many wireless SSID's are in scope for testing?

Answer: Refer to Answer No. 13.

**56.** Social Engineering

a) Would you like the penetration testing partner to attempt email discovery and then validate targets with CTPF, or would CTPF prefer to supply target email addresses?
b) How many email addresses should be targeted?
c) Spear phishing campaigns often involve the registration of new, bespoke domains per engagement and thus are likely to get caught in antispam controls. Is it acceptable to whitelist a source whitelist email address once the campaign(s) is built?

Answer:

a. Penetration testing partner to attempt email discovery
b. Approximately 300
c. No

**57.** Is the IT organization centralized or decentralized?

Answer: Signed NDA required for response

**58.** What is CTPF's budget for this project?

Answer: Please refer to Answer No. 44.

**59.** Has CTPF had this type of assessment performed in the past?

Answer: Yes

**60.** As an organization, are you confined to awarding to the lowest bidder?

Answer: No. The competitive solicitation was not advertised as a Request for Bids, but as a Request for Proposals which evaluates the written submissions for willingness, and ability to fulfill the scope of work. The contract award will be made to the most responsive and responsible bidder. The award will be based on various criteria with price being one of the variables.

**61.** External Network Penetration Testing

a) Approximately how many IPs are active?

b) Is exploit testing included in the external network vulnerability scans?

Answer:

a. Number available upon signing NDA agreement

b. Yes

**62.** Internal Network Penetration Testing

Approximately how many IPs or subnets are in scope?

7880 addresses over 31 Subnets

Can all internal network testing be done from a single location?

Yes, if security protocols and ACLs are removed as needed.

Answer: See above.

**63.** Firewall Assessment

a. Excluding redundant or firewalls running in HA mode, how many firewalls are in scope?

Answer: 1

**64.** Web Applications

a. How many web applications are in scope?

b. Are the web applications Internet-facing or internal only?

Answer:

a.3

b. Combination

**65.** Wireless Security Scanning

a. Is the wireless network controller-based or access-point-based?

b. How many locations are in scope for wireless network testing?

Answer:

a. Network controller-base

b. 1 location, 2 separate floors

**66.** Social Engineering

a. How many targets are anticipated for each type of testing?

b. How many locations are anticipated for physical security testing?

Answer:

a. There are approximately 200 employees and contractors so the targets would be a subset of that number.

b. 1 location, 2 separate floors.

**67.** What type of defensive cybersecurity technologies are currently in place?

Answer: 66 (a) Refer to Answer No. 56.

**68.** Can you provide an approximate number of external/public IP address ranges in scope for the testing?

Answer: Refer to Answers Nos. 1 and 2.

**69.** How large are the external ranges?

Answer: 265 addresses

**70.** What is the population of live devices in these ranges?

Answer: Approximately 40 IPs

**71.** Are devices hosted in cloud environments? Is it multi-tenant?

Answer:

1. There are virtual devices hosted in cloud environments.
2. All is multi-tenant.

**72.** Are there any 3rd party hosted IPS/ranges included in the scope?

Answer: Yes

**73.** Are there any IPs we should refrain from scanning?

Answer: An IP exclusion list will be provided.

**74.** Can Internal Pentest work be completed remotely or is an on-site presence mandatory?

Answer: There is no mandatory requirement.

**75.** What is the approximate breakdown of the number of internal devices that are in scope?

a. Total number of Subnets
b. Servers
c. Workstations
d. Firewall / Routers / Switches
e. Wireless Access Points / Controllers
f. Network segments

Answer:

a. 32
b. 180
c. 250
d. 30
e. 19
f. 32

**76.** Is the entire in scope internal network accessible from one logical connection

a. If not, approximately how many physical locations are in scope for onsite visits?

Answer:  Yes

**77.** How many data centers do you have? Are any hosted by 3rd party?
Answer:  No data centers

**78.** What kind of IoT devices are set up within the environment?
Answer:  Cameras, environmental monitoring devices

**79.** Is the network segmented? How many VLANs are there?
Answer: Yes, 32

**80.** How many web applications are included in the assessment?
Answer: See 5 and 6

**81.** For each application, please provide details on the number of user forms, web servers, database servers, and application servers.
Answer: See 26 for application size. Each application will have a single database server and application server.

**82.** Are there any restricted timeframes for testing web applications?
Answer:  No

**83.** For authenticated-based testing, specify the number of user types to be tested for each application.

Answer: See 6

**84.** Can you provide the number of separate facilities/buildings with separate wireless networks?
Answer: Refer to Answer No. 15.

**85.** How many access points in scope?
Answer:  19

**86.** How many SSIDs in scope?
Answer: Refer to Answer No. 13.

**87.** How many physical locations to test the wireless network? Where are the physical locations/departments?
Answer: Refer to Answer No. 15.

**88.** Provide details on the number of email IDs to be targeted for phishing assessments.
Answer:  300

**89.** How many phishing scenarios are in scope?

Answer: Refer to Answer No. 14.

**90.** Provide details on the number of locations in scope for physical impersonation or piggybacking assessments.

Answer: 1

**91.** Would you assist in whitelisting IP addresses for phishing campaign should the emails get held in Spam?

Answer: No whitelisting permitted

**92.** Are phone calls or pretext assessments (Vishing) in scope?

Answer: Yes

**93.** Are testing of applications required for regulatory compliance programs? If yes, please specify the programs.

Answer: HIPAA

**94.** Has the organization conducted a third-party network Pentest / vulnerability assessment previously? If yes, provide the assessment date.

Answer: Yes, annually

**95.** Are there documented security policies, procedures, standards, application data flow diagrams, database schemas, and network diagrams available?

Answer: Yes

**96.** For the purposes of disclosures related to item (iii) on pages 14 through 17, please confirm whether disclosure from the respondent is required only for the organizations listed on pages 15 and 16.

Answer: Please review and follow the instructions contained in the RFP requesting the information in section (iii), particularly the statement "The Trustees have determined that the following organizations presently fall under this required disclosure:"

**97.** May we provide a continuous Platform service for Red Teaming as a Service?

Answer: No

**98.** What is the estimated start date?

Answer: After the vendor is selected, Internal Audit will work with the vendor and CTPFs IT Department to determine the start date of each planned project.

**99.** May we provide a Firm Fixed Price (FFP) instead of Hourly by assessment type?

Answer: Please follow the RFP instructions.

**100.** For the External Network:

1. How many IP addresses?

2. How many domains?
3. Is the firewall assessment to check which ports are allowed?
4. Or do you want a more in-depth configuration assessment?

Answer: Please refer to Answers Nos. 1 and 2.

**101.** For the Internal Network:

1. How many in-scope IP addresses?
2. Is there a Windows domain

Answer: Answer: Please refer to Answers Nos. 1 and 2.

**102.** For the CTPF Web Application:

1. How many separate web applications?
2. How many API endpoints and pages for each application?
3. Will source code be provided?

Answer: Please refer to Answers:

1. See 5 and 6
2. See 28
3. No

**103.** For Wireless:

1. How many sites must be assessed?
2. Where is each site located?

Answer: 1 site, 2 separated floors.

**104.** For the Social Engineering Assessment:

1. How many phishing campaigns must be executed? Refer to Answer No. 34
2. How many employees will be targeted? Refer to Answers Nos. 35 and 36
3. Will Multi-Factor Authorization (MFA) bypass be expected/desired? Expected.
4. If so, what MFA technology is in use? Details available with a signed NDA.

Answer: See Answers provided above.

**105.** For the Physical Assessment:

1. How many sites will be assessed?
2. How many floors does each site contain?
3. What is the location at each site?
4. Will building security be informed beforehand?
5. Will local law enforcement be informed beforehand?
6. Will assessors be given documentation that their activities are allowed?
7. Are non-destructive lock-picking techniques allowed?

Answer:

a. 1

b. 2

c. Chicago

d. No

e. No

f. Yes

g. Yes

**106.** What is the approximate number of Internet-facing IP addresses for the external network assessment?
Answer: See question 2.

**107.** Does CTPF employ a DMZ or External Transit Network (VLAN with public subnet)?
Answer: Yes

**108.** What is the model of your firewall?
Answer: Cisco

**109.** What is the number of web applications to be assessed?
Answer: See 5

**110.** For each web application, what is the number of interactive pages per app (pages with data entry, dynamically generated content retrieval/presentation, API connections to data stores, etc.)?
Answer: Please refer to Answers Nos. 26 and 28.

**111.** How many SSIDs need to be tested?
Answer: Refer to Answer No. 13.

**112.** How many locations will be included in the assessment?
Answer: 1 location, two separate floors.

**113.** Does CTPF have systems in public clouds, such as AWS and Azure that need to be included in any assessment?
Answer: Yes

**114.** How many Internet facing hosts comprise the in-scope environment (servers, routers, firewalls, IDS/IPS)?

    - # Servers in scope?
    - How many firewalls/switches/routers?
    - IDS/IPS – do you utilize one and if so, is it locally managed?
- How many Internet facing sites/applications (URLs) are included in the scope? Please refer to Answer No. 5
    - How many websites are in-scope? Please refer to Answer No. 5
    - Do you want web applications assessed? Yes
- If so, how many web applications? Please refer to Answer No. 5
    - Would you like any applications tested without credentials? Yes
    - Would you like any applications tested with regular credentials? Yes
    - Would you like applications tested with admin credentials? Yes

Answer: Please see answers provided above.

**115.** Please list all internal network segments in scope (management, production, development, DMZ, etc.).

Answer: There are about 32. Details regarding network segmentation available with a signed NDA.

**116.** Please list any persistent connections to 3rd-party vendors (HVAC, IT service provider, etc.) that are in scope.

Answer:

1. NOC NAT tunnel over IPSEC
2. Two Cisco Umbrella tunnels for SIG

**117.** Do you want any cloud environments tested such as Azure or Amazon Web Services?

Answer: Yes.

**118.** Are there any remote access services in-scope (on-demand VPN, GoTo my PC, LogMeIn, etc.)?

Answer: VPN.

**119.** How many employees have remote access?

Answer: All 150 employees and many contractors have remote access.

**120.** Are there any in-bound modems (or remote access) in use?

Answer: Yes. Details available upon signing an NDA.

**121.** How many servers in-scope?

- Windows servers?
- Other operating systems (please list)?

Answer: Windows, Linux approximately 180 altogether.

**122.** How many users?

Answer: 200 user accounts.

**123.** What database technologies are in use (Oracle, Microsoft SQL, IBM DB2, MySQL, PostgreSQL, etc.)?

Answer: MS SQL.

**124.** Has the organization performed any Social Engineering exercises? Do you want one?

Answer:

a. No

b. Yes

**125.** How many locations/buildings are included for a physical assessment, if any?

Answer: 1 location, 2 separate floors

**126.** Is there a formally adopted security framework in use?
Answer: Proposal should identify which security framework the pen test will use.

**127.** How many sites to be included in the wireless assessment?
Answer: 1 location, 2 separate floors.

**128.** How many wireless users do you have?
Answer: 150

**129.** How many wireless networks are in-scope?
Answer: 1 SSID's

**130.** Do you have cybersecurity policies currently and if so, how many exist?

Answer: There are multiple cybersecurity policies.

**131.** How many different phishing attacks are in-scope?
Answer: All are in scope.

**132.** How many locations are included in the physical access assessment?
Answer: Refer to Answer No. 15.

**133.** Do you want the physical assessment to include penetration of the building, review of the internal physical security of the location, or both?
Answer: Please refer to Answer No. 44.

**134.** What is the budget for this project?
Answer: Please refer to Answer No. 44.

**135.** Are we to include the "2022-EEOC-Employees-Final" document as a separate attachment or would you like for it to be embedded within our proposal?
Answer: Please submit as attachment with an accurate label.

**136.** Number of live IP's exposed to the internet (not asking for the whole range of IP's owned; just a count of how many are actively being used).
Answer: Number available upon signing NDA.

**137.** Number of separate locations / disconnected networks in scope.
Answer: 1 production location, one DR site network.

**138.** Number of live IP's on each internal network (includes any IP's being used, such as phones, printers, etc. in addition to servers and workstations).
Answer: Detailed answer available upon submitting signed NDA.

**139.** Number of unique applications are in scope

For EACH application:

a. Number of dynamic pages (those that respond to user input)
b. Number of user roles, if authenticated testing

Answer: Please refer to Answers Nos. 5, 6, 26, and 28.

**140.** Number of locations

a. For EACH location, number of SSID's

Answer: 2 SSID's altogether.

**141.** Number of locations for physical penetration testing

a) Number of phishing targets for one scenario

Answer: 1 location.