財團法人中華民國證券暨期貨市場發展基金會弱點掃描服務委外服務案建議書徵求文件

目 次

壹、專案概述

一、專案名稱

財團法人中華民國證券暨期貨市場發展基金會「弱點掃描服務」委外服務案（以下簡稱本案）。

二、專案目標

藉由本案之執行成果，以檢測受測目標之資安防護能力與發現潛在作業系統弱點，並依據檢測結果提出改善建議，協助受測目標提升系統安全防護成效。

三、專案範圍

本案的服務範圍設備清單詳見附件1。

四、專案期間

自簽約日起 六個月 止。

貳、專案工作項目

得標廠商針對機關Web 主機或電腦系統進行安全弱點掃描，評估掃描標的物是否存在安全弱點，同時提供相關掃描結果，作為主機資訊安全的管理依據，並協助弱點修補方法之參考建議，待修正弱點後提供複掃，以確認弱點已經排除。

一、掃描內容

弱點掃描分為系統弱點掃描與網站弱點掃描。

(一)系統弱點掃描

係針對作業系統的弱點、網路服務的弱點、作業系統或網路服務的設定、帳號密碼設定及管理方式等進行弱點檢測，系統弱點掃描的檢測項目須符合Common Vulnerabilities and Exposures (CVE)發布的弱點內容(最新版)，至少包含以下項目：

1.作業系統未修正的弱點掃描

2.常用應用程式弱點掃描

3.網路服務程式掃描

4.木馬、後門程式掃描

5.帳號密碼破解測試

6.系統之不安全與錯誤設定檢測

7.網路通訊埠掃描

(二)網站弱點掃描

係針對機關對外主機網頁安全弱點進行掃描，檢測項目須符合最新版OWASP TOP 10 2017 的項目：

31.A1:Injection

2.A2:Broken Authentication

3.A3:Sensitive Data Exposure

4.A4:XML External Entities (XXE)

5.A5:Broken Access Control

6.A6:Security Misconfiguration

7.A7:Cross-Site Scripting (XSS)

8.A8:Insecure Deserialization

9.A9:Using Components with Known Vulnerabilities

10.A10:InsufficientLogging&Monitoring

(三)執行方式

1.得標廠商應於需求訪談階段先分就本機關之網路架構及本項服務之標的設備進行了解，如設備廠牌、系統版本等，以利後續進行弱點分析及修補建議。

2.掃描工具為取得授權使用的商用軟體，於每次弱點掃描前，將工具之弱點資料庫更新至最新版本，並應提供佐證資料，以確保本項服務之完整正確。

3.得標廠商應依排定之日期執行弱點掃描，於非公務時段或與機關協調取得適當時間進行掃描作業。

4.得標廠商應於弱點初掃後協助本機關進行弱點修補，針對應修補之弱點進行追蹤管理，包括彙整本機關之弱點修補情形，維護未修補清單中之未修補或排除原因等。

參、管理需求

一、廠商資格

為確保資訊安全及得標廠商所提供的服務水準，得標廠商應符合下列條件，並於服務建議書專章詳述：

(一)凡在政府機關登記合格，無不良紀錄之廠商（檢附設立及登記證明、納稅證明及信用證明）且不得為陸資企業(包括子公司、分公司、獨資或合夥事業及其轉投資事業)。本案服務人員需具有中華民國國籍，不得為外籍勞工或大陸來台人士。

(二)本案服務內容涉及敏感資訊，得標廠商不得轉包或分包予其他廠商執行。

(三)投標廠商須實施資訊安全管理制度，通過ISO 27001:2013 或其他類似驗證，並於專案執行期間持續有效，以保護弱點掃描服務所取得之資料。

(四)本案團隊人力至少應包含專案負責人/專案經理與弱點掃描服務人員。弱點掃描服務人員應具備以下所列舉之技能，且各類技能至少有一名成員，以確保服務水準，並於建議書中檢附成員姓名、訓練證書或專業證照等影本以供審核。應具備必要資訊網路、系統技能說明如下:

1.熟悉弱點掃描工具與掃描結果判讀能力，接受過CEH(Certified Ethical Hacker)或其他類似相關課程訓練。

二、服務水準協定(SLA)與罰責

(一)服務水準規範

本案各項服務水準協定（Service Level Agreement，SLA），以必須達成該項工作服務項目要求為依據，透過客觀的證據或指標，做為品質管制，以預防各項不符合作業的事項發生，降低委外作業的風險， 詳細服務水準規範如下表：

項次	項目	服務水準
1	執行時程	初掃：每次以2 週為限 複掃：每次以2 週為限 檢測報告：初掃及複掃結束後2 週內提供
2	設備服務中斷時間	因執行弱點掃描服務造成軟硬體設備服務中斷時，應協助機關恢復正常運作，服務中斷時間不得超過8小時

(二)相關說明：

1.承作廠商無法達成相關工作項目要求或交付文件，其罰款(違約金)計算方式為每延遲1 日(以日曆天計，星期日、國定假日及其他休息日均應計入，不滿1 日以1 日計算)，本機關得按契約總價之千分之一計算懲罰性違約金，款項可自契約總價或履約保證金項中扣抵。

2.違約金上限依採購法之採購契約要項第四十五點規定，違約金以契約總價之20%為上限。如違約金逾20%時，本機關得以書面通知得標廠商終止契約或解除契約之部分或全部，且不補償得標廠商所生之損失。

3.得標廠商應於議價後所提成本分析中，詳列各項工作項目成本，如於驗收時，經審查發現有不合格之工作項目，得標廠商應依期限予以改正。如未改正，本機關有權扣除該項工作之款項。

4.得標廠商指派之專案負責人及工作成員，未經本機關同意，不得更換，如有未經本機關同意自行更換時，每更換乙次得依契約總價之

千分之一計算懲罰性違約金。

三、品質需求與驗收標準

(一)品質需求

1.為確保專案如期如質完成，廠商應針對本專案之需求，妥慎成立專案小組，執行本專案所需之各項作業，並指派專案經理負責督導工作項目。

2.得標廠商訂定品質管理流程，本機關得以稽核。

3.得標廠商於專案期間應辦理啟始會議與結束會議，並視情況召開專案管理會議以掌控品質，會議討論內容與結果需作成紀錄與追蹤辦理，送本機關備考。

(二)驗收標準

得標廠商應依貳、專案工作項目之服務需求，以及符合服務水準協定(SLA)中所列事項，完成專案工作，並依本說明文件所訂之交付時程，完成相關文件與紀錄之交付。

(三)驗收方式

本機關將於各項工作項目交付完成後進行審查作業，得標廠商需依本機關審查意見修正交付項目，並再送至本機關複驗。

四、業務保密安全責任

(一)廠商基於本案需要，所取得各種形式之資訊，包含文書、圖片、紀錄、照片、錄影（音）及電腦處理資料等，可供聽、讀、閱覽或藉助科技得以閱讀或理解之文書或物品，應負資訊保密及確保資訊安全責任， 並簽定保密協議書。

(二)廠商對特別以文字標示或口頭明示為機密資料者，非經本機關書面同意，不得洩漏資料予第三者，致使造成之法律責任或賠償，廠商應負完全責任。

(三)廠商對於可能接觸與本案相關資料或文件之人員，須提供保密管理機制，相關人員均須簽署保密切結書(切結書形式由廠商自訂)。

(四)契約終止時，廠商應將有關本案過程中處理之任何形式資訊，整理歸檔後退還本機關或經本機關同意後銷毀。

(五)履約期間造成保密及安全事件，得歸咎於廠商之責任時，廠商應負所有法律及賠償責任。

(六)本機關對廠商保留實地稽核權，以確保廠商於委外服務期間與合約終止時之資料安全、設備管理及其他安全維護事項已採取必要措施。

肆、交付項目

一、交付項目與時程

(一)工作計畫書：決標日起2 週(日曆天)內交付。

(二)弱點掃描服務中文報告：依工作計畫書載明之交付時程。

(三)弱點複掃服務中文報告：依工作計畫書載明之交付時程。

二、交付文件格式

(一)各項文件應提供紙本 3 份，電子檔 3 份（以光碟或本機關同意之儲存媒體及提交方式）。

(二)必要時本機關得要求派員親臨說明。

三、交付項目說明

交付項目	內容說明
1. 工作計畫書	▪工作計畫書應以廠商投標時之「建議書」為基礎，並依採購評選意見修改 ▪內容除包括對本專案之執行敘述，含專案管理、組織、人力(須含專業認證證明)、分工、職掌、工具(須含授權)、工作項目、執行掃描方式、時程(須含初掃、弱點修補、複掃、報告提交等)、工作進度稽核點及品質管理流程
2. 弱點掃描服務中文	▪ 文件內容應包括：執行結果摘要說明、專案執行計畫(執行期間/執行項目/執行範圍/專案成員)、掃描工具說明、掃描方式、弱點統計(依風險等級、弱點類別排序)、弱點清單(弱點名稱、弱點描述、設備名稱、IP/URL、Portname、風險等級、修補建議)、掃描誤判之弱點清單(說明誤判理由)、弱點排除清單(說明排除理由，如無法修補原因與配套措施)。

交付項目	內容說明
3. 弱點複掃描服務中文報告	▪ 文件內容應包括：執行結果摘要說明、專案執行計畫(執行期間/執行項目/執行範圍/專案成員)、掃描工具說明、掃描方式、弱點統計(依風險等級、弱點類別排序)、弱點清單(弱點名稱、弱點描述、設備名稱、IP/URL、Portname、風險等級、修補建議)、掃描誤判之弱點清單(說明誤判理由)、弱點排除清單(說明排除理由，如無法修補原因與配套措施)、與初掃之差異化報表(例如未修補弱點及新發現弱點等相關描述與統計)。

伍、建議書製作規定

一、服務建議書格式

(一)紙張：宜用A4 規格。

(二)繕打及裝訂方式：由左至右橫式繕打，加註頁碼，加裝封面及目錄，封面上註明廠商名稱、廠商地址、本案名稱及日期，裝訂線在左側。

(三)目次：應標示各章節之出處頁碼。

(四)廠商投標建議書之份數為1 式 3 份。

二、服務建議書內容

(一)專案概述

1.專案名稱

2.專案目標

3.專案時程

(二)廠商說明

1.廠商簡介

2.公司營運狀況，包含參與人員名單、能力證明及廠商經驗說明

(三)專案計畫

1.專案服務內容項目

2.組織與人力配置

3.專案時程、品質、風險管理與交付項目計畫，包含工作項目、時程規劃及查核點

4.本案帶來之預期效益

5.本案SLA 之承諾

(四)其它

陸、附件

附件1 弱點掃描服務範圍設備清單

例如：

項目	掃描類別	IP / URL	設備種類(如主機/伺服器種類、通訊設備種類、個人電腦等)	備註 (如設備廠牌、系統版本)
1	主機弱點掃描	14		
2	網站設備弱點掃描	6		
	…			