

政府機關資安健診服務委外服務案  
建議書徵求文件(範本)  
(V4.0)

行政院國家資通安全會報技術服務中心  
中華民國110年9月

## 修訂歷史紀錄

版次	發行修訂生效日期	變更說明
▪ 第 1.0 版	▪ 102 年 12 月 25 日	▪ 新版正式發行
▪ 第 2.0 版	▪ 103 年 11 月 1 日	<ul style="list-style-type: none"> <li>▪ 封包監聽與分析、網路設備紀錄檔分析及防火牆連線設定，增加服務內容要求</li> <li>▪ 強化報告架構與內容要求</li> </ul>
▪ 第 3.0 版	▪ 107 年 1 月 16 日	<ul style="list-style-type: none"> <li>▪ 增修使用者端電腦檢視內容項目，對使用者電腦更新檢視之電腦組態設定，依行政院國家資通安全會報技術服務中心，官方網站「政府組態基準」為檢視基準，及強化檢測內容項目說明。</li> </ul>
▪ 第 4.0 版	▪ 110 年 9 月 15 日	<ul style="list-style-type: none"> <li>▪ 調整工作項目與資安法之資安健診項目名稱一致</li> <li>▪ 移除使用者電腦 GCB 檢視</li> <li>▪ 新增停用作業系統之版本</li> <li>▪ 調修專案人員資格</li> <li>▪ 新增限制廠商使用大陸廠牌之資通訊產品及因服務所利用或產生資料之保護</li> </ul>
▪	▪	▪
▪	▪	▪

# 目次

壹、 專案概述 .....	1
一、 專案名稱 .....	1
二、 專案目標 .....	1
三、 專案範圍 .....	1
四、 專案期間 .....	1
貳、 專案工作項目 .....	2
一、 網路架構檢視 .....	2
二、 有線網路惡意活動檢視 .....	2
三、 使用者端惡意活動電腦檢視 .....	2
四、 伺服器主機惡意活動檢視 .....	3
五、 目錄伺服器設定檢視 .....	4
六、 防火牆連線設定檢視 .....	4
參、 管理需求 .....	5
一、 廠商資格 .....	5
二、 服務水準協定(SLA)與罰責 .....	7
三、 品質需求與驗收標準 .....	9
四、 業務保密安全責任 .....	10
五、 專案經費預算金額 .....	10
肆、 交付項目 .....	12
一、 交付項目與時程 .....	12
二、 交付文件格式 .....	12
三、 交付項目說明 .....	13
伍、 建議書製作規定 .....	14
一、 服務建議書格式 .....	14

二、 服務建議書內容.....	14
陸、 建議書評選事宜.....	16
一、 評選辦法.....	16
二、 評選標準.....	17
三、 其他評選注意事項.....	18

## 壹、專案概述

### 一、專案名稱

「資安健診服務」委外服務案（以下簡稱本案）。

### 二、專案目標

期透過本案整合各項資訊安全項目的檢視服務，提供資安改善建議，以提升政府網路與資訊系統安全防護能力。

### 三、專案範圍

本案的服務範圍包括網路架構檢視、有線網路惡意活動檢視、使用者端電腦檢視、伺服器主機檢視、目錄伺服器設定檢視、防火牆連線設定檢視等資安專業服務。

### 四、專案期間

自簽約日起至 XXX 年 XX 月 XX 日止。

## 貳、專案工作項目

資安健診服務內容應涵蓋以下所列的所有服務項目，廠商應具備完成各項服務所需之軟、硬體設備，專案執行期間需提供 5x8 小時之專案諮詢服務，並配合機關辦理說明會議。

### 一、網路架構檢視

針對本機關網路架構圖進行安全性弱點檢視，檢視之項目包含設計邏輯是否合宜、主機網路位置是否適當及現有防護程度是否足夠。

### 二、有線網路惡意活動檢視

#### (一)封包監聽與分析

在本機關有線網路(內網、外網、DMZ 區或 N 個網段)適當位置架設側錄設備，觀察內部電腦或設備是否有對外之異常連線或 DNS 查詢，並比對是否連線已知惡意 IP、中繼站(Command and Control, C&C)或有符合惡意網路行為的特徵。發現異常連線之電腦或設備需確認使用狀況與用途。

#### (二)網路設備紀錄檔分析

檢視網路與資安設備共 N 台(如防火牆、入侵偵測/防護系統等)紀錄檔，分析過濾內部電腦或設備是否有對外之異常連線紀錄，發現異常連線之電腦或設備需確認使用狀況與用途。

### 三、使用者端惡意活動電腦檢視

#### (一)使用者端電腦惡意程式或檔案檢視

針對個人電腦共 N 台進行是否存在惡意程式或檔案檢視，檢視項目包含活動中與潛藏惡意程式、駭客工具程式及異常帳號與群組。

## (二)使用者電腦更新檢視

1. 針對使用者電腦共 N 台進行作業系統更新情形。
2. 使用者電腦安裝之 Microsoft 各項應用程式安全性更新，包含 Office 應用程式、Adobe Acrobat、及 Java 應用程式更新檢視。
3. 檢視使用者電腦是否使用已經停止支援之作業系統或軟體(如 Windows XP、Windows7、Office 2003、Office 2007、Adobe Flash Player 等)
4. 針對使用者電腦防毒軟體安裝、更新及定期全系統掃描狀況進行檢視。

## 四、伺服器主機惡意活動檢視

### (一)伺服器主機惡意程式或檔案檢視

針對伺服器主機共 N 台進行是否存在惡意程式或檔案檢視，檢視項目包含活動中與潛藏惡意程式、駭客工具程式及異常帳號與群組。

### (二)伺服器主機更新檢視

1. 檢視伺服器主機共 N 台進行作業系統更新情形。
2. 檢視伺服器主機安裝之 Microsoft 各項應用程式安全性更新，包含 Office 應用程式、Adobe Acrobat、及 Java 應用程式更新
3. 檢視伺服器是否使用已經停止支援之作業系統或軟體(如 Windows XP、Windows7、Windows Server 2008、Windows Server 2008 R2 Office 2003、Office 2007、Adobe Flash Player 等)
4. 檢視伺服器是否使用不合宜之作業系統(如使用 Windows10 等)。
5. 針對伺服器主機防毒軟體安裝、更新及定期全系統掃描狀況進行檢視。

## 五、目錄伺服器設定檢視

檢視 N 台目錄伺服器中，針對 AD 伺服器組態設定，依行政院國家資通安全會報技術服務中心，官方網站「政府組態基準」專區所公布安全性檢視之內容為主，以確認機關對於組態設定之落實情形。參考網址為 <https://www.nccst.nat.gov.tw/GCB>。

若無 AD 伺服器，可以其他目錄伺服器(如 LDAP)或以個別使用者端電腦檢視方式完成「密碼設定原則」與「帳號鎖定原則」安全設定檢視(使用者端電腦以項次三的電腦為範圍)。

## 六、防火牆連線設定檢視

檢視 N 台防火牆的連線設定規則(如外網對內網、內網對外網、內網對內網)是否有安全性弱點，確認來源與目的 IP 與通訊埠連通的適當性 (包含設置「Permit All/Any」與「Deny All/Any」等 2 項防火牆檢測規則確認)。

## 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)本案服務內容將涉及敏感資訊，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 版或其他類似驗證，並於專案執行期間持續有效，以保護資安健診所取得之資料。
- (四)本案涉及資通訊軟體、硬體或服務等相關事務，不得提供及使用大陸廠牌資通訊產品，服務如涉及使用雲端工具，應確保機關利用服務之所屬一切資料存取、備份、及備援之實體所在地，應為我國管轄權所及之境內。
- (五)本案團隊人力至少應包含專案負責人/專案經理與資安健診服務人員。每位資安健診服務人員應依服務項目，具備擇 1 證照，以確保服務水準，並於建議書中檢附成員姓名、員工證明(勞健保證明)、專業證照等影本以供審核。

(1) 網路架構檢視、防火牆連線設定檢視：擇 1 證照

➤ CCNA(Cisco Certified Network Associate)。

- CCNP Security(Cisco Certified Network Professional Security)。
- CND(EC-Council Certified Network Defender)。
- CompTIA Network+。
- iPAS 資訊安全工程師中級能力鑑定。
- 其他相關資安證照。

(2) 網路(有線)、使用者端電腦、伺服器主機等惡意活動檢視：  
擇 1 證照

- CEH(Certified Ethical Hacker)。
- CHFI(Computer Hacking Forensic Investigator)。
- CND(EC-Council Certified Network Defender)。
- SSCP(System Security Certified Practitioner)。
- CompTIA Security+。
- 其他相關資安證照。

(3) 目錄伺服器設定檢視：擇 1 證照

- Microsoft Certified: Azure Administrator Associate。
- Microsoft Certified: Azure Security Engineer Associate。
- CompTIA Security+。
- SSCP(System Security Certified Practitioner)。
- iPAS 資訊安全工程師中級能力鑑定。

➤ 其他相關資安證照。

## 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	網路架構檢視	<ul style="list-style-type: none"><li>▪ 檢視內容需包含網路架構部署表現(網路架構設計、電腦設備配置、備援機制)、網路邊界安全管理(防火牆管理、存取控制)及網路設備安全表現(登入認證機制、安全性更新)</li></ul>
2	封包監聽與分析	<ul style="list-style-type: none"><li>▪ 在有線網路適當位置架設側錄設備，進行封包側錄至少以 6 小時為原則，以觀察是否有異常連線</li><li>▪ 封包側錄檔案的可用性達 100%</li></ul>
3	網路設備紀錄檔分析	<ul style="list-style-type: none"><li>▪ 網路設備紀錄檔分析以 1 個月或 100 Mbyte 內的紀錄為原則</li></ul>
4	使用者端電腦惡意程式或檔案檢視	<ul style="list-style-type: none"><li>▪ 惡意程式檢測時，使用者電腦故障率需小於 1%</li><li>▪ 因惡意程式檢測所造成的使用者電腦故障，需於 10 分鐘內完成通報，8 小時內修復完成</li></ul>

項次	項目	服務水準
5	使用者電腦更新檢視	<ul style="list-style-type: none"> <li>更新狀態需追蹤至實地檢測前 1 個工作日</li> </ul>
6	伺服器主機惡意程式或檔案檢視	<ul style="list-style-type: none"> <li>惡意程式檢測時，伺服器主機故障率需小於 1%</li> <li>因惡意程式檢測所造成的伺服器主機故障需於 10 分鐘內完成通報，24 小時內修復完成</li> </ul>
7	伺服器主機更新檢視	<ul style="list-style-type: none"> <li>更新狀態需追蹤至實地檢測前 1 個工作日</li> </ul>
8	目錄伺服器設定檢視	<ul style="list-style-type: none"> <li>檢視目錄伺服器(如 MS AD)組態設定，提出與政府組態設定規定之符合情形，並提出檢視報告</li> </ul>
9	防火牆連線設定	<ul style="list-style-type: none"> <li>防火牆開啟通訊埠檢視範圍需涵蓋 0~65535</li> </ul>

(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。
- 5.得標廠商應將文件品質保證納入專案品質保證項目，嚴謹製作本專案各項文件，包含版面及內容皆須嚴格要求一致性及正確性。交付本機關之文件經本機關審閱時，所發現錯漏處達N處以上，或業經本機關要求修訂仍未修訂者，本機關得按每字新台幣XXX元計算懲罰性違約金，並自付款項中扣抵；其有不足者，得通知廠商繳納或自履約保證金扣抵。

### 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，須提供保密管理机制，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。

## 五、專案經費預算金額

(一)本案 XXX 年度預算金額為新台幣 XXX 萬元整。

(二)本案所須之人力由得標廠商自由運用調配，並於建議書中詳述計費標準與成本分析。

## 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)資安健診服務報告：依工作計畫書載明之交付時程。
- (三)專案執行紀錄檔：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 N 份，電子檔 N 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	<ul style="list-style-type: none"> <li>▪ 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</li> <li>▪ 內容除包括對本專案之執行敘述，含專案管理、組織、人力、分工、職掌、工作項目、執行情序(網路/個人電腦/伺服器)、時程說明(包括起始會議與結束會議)、受測機關檢測範圍與影響、受檢測機關準備事項、工作進度稽核點及品質管理流程</li> <li>▪ 受檢測機關準備事項建議包括：受測個人電腦清單(IP、所安裝之作業系統與應用程式)、受測伺服器清單(IP、用途、所安裝之作業系統與應用程式、管理人員)、網路架構圖(標示部署設備位址)、網路設備紀錄檔、協同檢測人員名單</li> </ul>
2. 資安健診服務報告	<ul style="list-style-type: none"> <li>▪ 文件內容應包括：執行結果摘要說明(依照檢測類別各別摘要說明)、執行計畫(執行期間/執行項目/執行範圍/專案成員)、執行情形(需包含所有服務項目執行結果，不可直接以工具產生之原始結果交付)、改善建議、結論</li> </ul>
3. 專案執行紀錄檔	<ul style="list-style-type: none"> <li>▪ 文件內容應包括：各個人電腦的資安檢測結果表、各伺服器主機的資安檢測結果表、網路側錄封包資料、發現惡意行為或惡意程式的過程紀錄(如果有發現)、外洩資料列表(如果有發現)、惡意程式(如果有發現)</li> </ul>

## 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 N 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、建議書評選事宜

### 一、評選辦法

- (一)依據「政府採購法」第 22 條第 1 項第 9 款之規定辦理，透過書面審查及簡報答詢的方式，以合於招標文件，標價合理且在預算金額內，經評選委員評選為合格的廠商，依序議價。
- (二)由本機關邀集專家學者組成評選委員會，除對廠商之建議書進行書面審查外，並由本機關召開評選會議，由廠商提出 15 分鐘對建議書之簡報，其後並接受評選委員之詢問，答詢時間以不超過 10 分鐘為限，惟因評審委員詢問題目過多時，主席得酌以延長答詢時間。評選會議時間及地點，將於資格審查時當場宣布或另備文通知，而廠商之簡報順序，亦於資格審查時抽籤決定。
- (三)簡報及答詢結束後，各評選委員根據本徵求建議書說明文件第柒之二「評審項目」所列項目及配分評定各廠商名次及其是否為合格廠商（以總得分 XX 分(含)以上為合格）。
- (四)各評選委員評定結果不得有同名次或從缺情形。
- (五)過半數(含)評選委員評定為合格之廠商方列入排名與序分計算；另半數以上（含）評選委員評定不合格之廠商，視為不合格，若所有廠商均不合格時，主席應宣布廢標，重新辦理本案。
- (六)本案評選採序位法辦理，就各評審項目分別評定並換算為序位，再加總計算廠商序位，最低者為第 1 優先序位，次低者為第 2 序位，餘依此類推。
- (七)經評選委員會評定優勝廠商，依優勝序位，自最優勝者起，依序以議價方式辦理，但有二家以上廠商為同一優勝序位者，以建議書的

標價低者優先議價，若仍相同者，則擇獲得評選委員評定序位第一較多者決標；仍相同者，抽籤決定之。

(八)評選結果簽請首長或授權人員核定後，由本機關另定時間通知廠商依序辦理議價。

## 二、評選標準

本案由評選委員就廠商所提出建議書之內容，針對其經驗、能力與服務水準，依下列各項目及配分，予以評分，總分 100 分，得分總計達 XX 分(含)以上者為合格。

評審項目	評審項目內容	配分
廠商業績及履約能力	1.廠商人力規模、商譽 2.資安實績與相關技術經驗	20
專案管理	1.對本案工作內容之瞭解 2.進度時程控管、資料管制與品質保證 3.本案之團隊規模與專案負責人之經驗 4.本案團隊成員之專業證照符合程度	20
專案規劃完整性	1.本案要求之各項服務項目的執行專業性 2.本案要求之各項交付項目之完整性	30
成本合理性	本案規劃、執行、專案管理及報告撰寫等各項費用估算之合理性	20
簡報及答詢	廠商簡報與答詢內容是否清楚、完整	10
總分		100
是否合格		<input type="checkbox"/> 合格 <input type="checkbox"/> 不合格
名次序位		

### 三、其他評選注意事項

- (一)本機關得因故終止評選事宜，通知投標廠商領回建議書。
- (二)本文件未盡事宜，依據「政府採購法」相關規定辦理。