資通安全服務採購規範

一、第 1 組資安健診服務

資安健診服務係透過整合各項資通安全項目的檢視服務作業，提供受檢單位資安改善建議，藉以落實技術面與管理面相關控制措施，以提升網路與資訊系統安全防護能力。

（一）服務項目：

項次	項目		內容說明	單位	最低訂購數量	各項服務單位所需人天
1	網路架構檢視		針對網路架構圖進行安全性弱點檢視，檢視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	網路架構	1 式	1
2	有線網路惡意活動檢視	封包監聽與分析	針對有線網路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 封包側錄至少以 6 小時為原則，以觀察是否有異常連線	側錄設備	2 台	2

項次	項目		內容說明	單位	最低訂購數量	各項服務單位所需人天
3		網路設備紀錄檔分析	檢視網路與資安設備(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 網路設備紀錄檔分析以 1 個月或 100 M byte 內的紀錄為原則	網路設備	2 台	1
4	使用者端電腦檢視	使用者端電腦惡意程式或檔案檢視	針對個人電腦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	使用者電腦	20 台	0.3
		使用者電腦更新檢視	作業系統與使用者電腦安裝之 Microsoft 各項應用程式安全性更新作業系統、Office 應用程式、Adobe Acrobat、Adobe flash player 及 Java 應用程式更新檢視(包含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 或 Office 2003))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			
5	伺服器主機檢視	伺服器主機惡意程式或檔案檢視	針對伺服器主機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	主機伺服器	5 台	0.3

項次	項目		內容說明	單位	最低訂購數量	各項服務單位所需人天
		伺服器主機更新檢視	作業系統與伺服器主機安裝之Microsoft 各項應用程式安全性更新作業系統、Office 應用程式、Adobe Acrobat、Adobe flash player及Java應用程式更新檢視(包含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、Windows Server 2003 或 Office 2003)) 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			
6	安全設定檢視	使用者電腦組態設定檢視	針對使用者個人電腦組態設定，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」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	使用者電腦	20 台	0.5
7		網通設備組態設定檢視	針對網通設備 (如：Juniper Firewall、Fortinet Fortigate、無線網路)之組態設定安全檢測，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	網通設備	N/A	0.5

項次	項目		內容說明	單位	最低訂購數量	各項服務單位所需人天
8		應用程式伺服主機組態設定檢視	針對應用程式(如：Exchange Server2013) 之組態設定安全檢測，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	伺服器主機	N/A	0.5
9		目錄伺服器組態設定檢視	針對 AD 伺服器組態設定(如 MS AD)，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，可以其他組態設定檢視項目替代	目錄伺服器	1 台	0.5
10		防火牆連線設定	檢視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)	防火牆設備	1 台	0.5

註：請廠商與採購機關事先完成溝通與討論，在使用者電腦組態與目錄伺服器組

態檢視設定時，如有例外管理，除設定例外管理之組態項目，並以文件記錄修改的組態項目。

（二）計價方式：

項目	單位	各項服務單位所需人天	採購數量(例)	採購數量所需人天(單位人天*採購數量)	單項服務金額(採購數量所需人天*人天費率)
網路架構檢視	網路架構	1	1	1	
有線網路惡意活動檢視(封包監聽與分析)	側錄設備	2	2	4	
有線網路惡意活動檢視(網路設備紀錄檔分析)	網路設備	1	2	2	
使用者端電腦檢視	使用者電腦	0.3	20	6	
伺服器主機檢視	伺服器主機	0.3	5	1.5	
安全設定檢視	使用者電腦	0.5	20	10	
	網通設備	0.5	1	0.5	
	伺服器主機	0.5	1	0.5	
	目錄伺服器	0.5	1	0.5	
	防火牆設備	0.5	1	0.5	
資安健診服務總金額					

註：各項服務單位所需人天數為工作日，每日以 8 工作小時計。(所需人天為該項服務從規劃到完成之人天數，非實際到場人天)。

（三）計價方式說明：

資安健診服務應涵蓋所有服務項目，各服務項目的採購單位數量，不得少於第(一)款服務項目所列之各項目最低訂購數量。

資安健診服務價金為各單項服務金額的總和。服務總金額計算方式為:(各項服務單位所需人天*各項訂購數量=各項採購數量所需人數，並將各項採購數量所需人數加總合計後)*人天費率。人天費率為決標單價價格。

（四）資安健診服務人員資格：

參與資安健診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。資安健診服務人員，應具備必要之各類資訊網路、系統技能條件說明如下：

1、網路管理：接受過 CCNA(Cisco Certified Network Associate)或其他類似網路管理相關課程訓練證明。

2、惡意程式檢視：接受過 CEH(Certified Ethical Hacker)、CHFI (Computer Hacking Forensic Investigation)或其他類似相關課程訓練證明(以上訓練證明擇一)。

3、封包分析：接受過 NSPA (Network Security Packet Analysis)或其他類似相關課程訓練證明。

4、目錄服務：接受過 MCSE (Microsoft Certified Solutions Expert)或其他類似相關課程訓練證明。

5、資訊安全技術或管理：接受過 CISSP(Certified Information Systems Security Professional)、ISO/CNS 27001 Lead Auditor 或其他類似相關課程訓練證明(以上訓練證明擇一)。

為順利於履約前驗證服務人員資格條件，廠商應就上述資格條件先行確認合格，再檢附成員姓名、訓練證書、專業證照等影本報請適用機關審核同意後始得服務。

服務人員須年滿 18 歲，身體健康、無法定傳染病，且具有中華民國國籍，不得為外籍勞工或大陸來台人士。於履約期間內，廠商團隊成員不得同時受僱於大陸地區，或有於大陸地區執業、工作等情形。

（五）廠商應配合事項及交付項目：

1、資安健診服務報告。

2、側錄封包資料（燒錄至光碟或其他媒體裝置）。

3、服務紀錄檔（燒錄至光碟）。

4、發現之惡意程式。

5、檢視服務之項目／數量與採購項目／數量相符。

6、服務所需軟硬體設備由廠商提供。

7、配合適用機關辦理至少一次說明會議。

（六）文件報告基本要求：

1、執行結果摘要說明(依照檢測類別各別摘要說明)。

2、執行計畫

執行期間/執行項目/執行範圍/專案成員。

3、執行情形

針對以下項目,說明檢視結果,並針對所發現不符合事項或問題,說明其發生原因：

（1）網路架構檢視

依照網路架構安全設計、備援機制設計、網路存取管控、網路設備管理、主機設備配置等風險類型分別說明檢視結果。

（2）有線網路惡意活動

封包監聽與分析

說明內部電腦或設備是否有對外之異常連線或 DNS 查詢，發現異常連線之電腦或設備需確認使用狀況與用途。

網路設備紀錄檔分析

依檢視之網路設備為序，表列包括設備名稱、位置、異常行為及紀錄檔時間等資訊,發現異常連線之電腦或設備需確認使用狀況與用途。

（3）使用者端與伺服器端電腦惡意程式或檔案檢視,依檢視之使用者電腦或伺服器 IP 為序，分別說明檢視結果及發現之惡意程式檔名。

（4）作業系統、Office 應用程式、防毒軟體、Adobe Acrobat 及 Adobe flash player 應用程式更新情形,使用者端與伺服器端電腦均分別依檢視項目逐項詳列未更新之台數及比例數。

（5）針對使用者個人電腦、網通設備組態設定及應用程式伺服主機之組態設定進行安全性檢視,以確認機關對於組態設定之落實情形，並記錄測試結果。

（6）目錄伺服器(例如微軟的 AD)中群組的密碼設定與帳號鎖定原則。檢視設定之合理性，如密碼歷程、密碼最短有效期及帳號鎖定閥值為零,並針對目錄伺服器組態設定進行安全性檢視，以確認機關對於組態設定之落實情形，並記錄測試結果。

（7）防火牆連線設定檢視

檢視防火牆的連線設定規則,例如外網對內網、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，並表列說明需改善之規則名稱與檢視結果，檢視結果內容如可進行匿名登入、未啟用此服務、不需提供遠端連線等資訊。

4、結果建議

針對各項結果，可依問題發生原因，提出根因改善建議。

5、結論

6、附件

（1）使用者端電腦檢測結果清單。

（2）伺服器端電腦檢測結果清單。

（3）外洩資料列表。

（4）發現惡意行為或惡意程式的過程紀錄與說明。

（七）適用機關配合事項

1、提供網路架構圖，並安排相關人員接受訪談。

2、提供受測之使用者端電腦清單、伺服器清單及目錄伺服器等資訊。

3、提供欲檢視之網路設備紀錄檔，如防火牆、入侵偵測／入侵防護系統等。

4、提供群組原則(Group Policy)。

5、提供防火牆政策(Rule)與開啟通訊埠(Port)的資訊。

6、若檢視之使用者端電腦或伺服器主機，實地場所有多處，最多以 3 處為限，超過額度部分，機關可請廠商提出服務費用報價或於下單前約定超出之服務費用。

二、第 2 組 SOC 監控服務

第 1 項：SOC 監控服務-低流量

SOC 監控服務提供防毒軟體、網路防火牆、應用程式防火牆、APT 防護機制、電子郵件過濾機制及 IDS/IPS 等資安事件監控及分析統計報表。透過監控及分析，可將防毒軟體、網路防火牆、應用程式防火牆、APT 防護機制、電子郵件過濾機制及 IDS/IPS 等所產生的資安日誌，以系統化方式進行收集、關聯性分析後，定期產生報表，提供給客戶作為資訊安全的管理依據。

受監控的網路整體處理效能可達 900 EPS(Event Per Second)，為分析日誌種類，設備數量或以網路流量推算所得。機關訂購前可根據日誌種類 EPS 參考表，加總機關內擁有的資安設備 EPS，計算監控所需要的 EPS 總量。日誌種類 EPS 參考表：

日誌種類	型式	EPS
網路設備(路由器)		250
資安設備(Firewall 防火牆)	低階	300
	高階	500
資安設備(IDS)	低階	150
	高階	450
資安設備(IPS)	低階	250
	中階	300
	高階	500
資安設備(WAF 防火牆)	低階	300
	中階	400
	高階	1500
個人防毒(防毒伺服器，防毒閘道器)		150
網站主機	低階	300
	高階	500
代理伺服器		250
郵件伺服器		200
郵件管理過濾器		150
目錄伺服器		150

日誌種類	型式	EPS
檔案伺服器		150
資料庫伺服器		500
DNS 伺服器	低階	150
	高階	250

（一）服務說明

1、SOC 監控環境部署

（1）廠商應於機關訂購單通知之次工作日起算 30 個日曆天內，勘查機關現有網路環境與需求，提出部署建議報告，並部署監控必要之遠端偵測器(日誌收集或 SIEM 等事件收集器)，所部署之設備不得影響現有各項安全設備之正常運作。部署工作應包含事件收集設備安裝、網段部署、設定、系統調校與重要資安事件 Rule 導入等工作。

（2）發現事件收集設備故障，必須於 24 小時內修復完成或調換同等級以上之相容設備。

（3）全年故障次數、總時間與搶救恢復時限作為指標，全年故障次數不可超過 5 次，故障總時間不可超過 104 小時，每次須於 24 小時內完成修復。

（4）若部署設備之實地場所有多處，最多以 3 處為限，超過額度部分，機關可請廠商提出服務費用報價或於下單前約定超出之服務費用。

（5）若機關有調整監控設備部署之需求，最多全年不得超過 8 次，超過額度部分，機關可請廠商提出服務費用報價或於下單前約定超出之服務費用。

2、監控服務

（1）廠商應遵循行政院國家資通安全會報技術服務中心制定之「政府領域聯防監控作業規範」，通過連通測試作業，並協助機關回傳資安監控情資至指定之聯防監控平台。

（2）廠商所提供之監控服務系統可從被監控端取得不同來源的日誌，經後送回 SOC 進行交叉比對後，可歸納出疑似資安

事件或惡意軟體行為，能從警示系統產生工單、或者事件單由專業資安人員判斷是否為資安事件。

（3）監控事件經監控中心判斷資安事件時，應即以適當方式(以電話、傳真、手機簡訊、電子郵件等)通知機關資安連絡人，俾其依「資通安全事件通報及應變辦法」之規定於知悉資安事件 1 小時內進行資安事件通報。

（4）廠商應定期提供月報、季報予機關，俾其依「資通安全責任等級分級辦法」之相關規定提交監控管理資料。報告需提供以下內容：

A、事件通知或警訊發布統計

發生事件編號、事件名稱、事件處理結果。

持續追蹤的資安事件列表。

造成受監控設備停止或受影響時間。

受影響 IP 列表。

B、監控與警示系統監控情形

事件工單處理狀態與數量。

機關內員工連接中繼站(IP、DNS)數量。

惡意軟體攻擊類型說明與數量。

受攻擊服務統計圖表。

C、資安事件處理說明

處理紀錄說明。

提供防禦措施說明。

D、資安威脅預警情形

資安威脅預警公告。

資安威脅預警建議。

資安威脅預警諮詢。

E、評估建議改善項目

資安監控服務狀況報告，月報得以電子郵件或客戶服務網站等方式獲得，季報則須到府進行提報。

3、資安事件處理

（1）若發生資安事件，機關可向廠商提出事件處理服務需求，處

理件數共 3 件，若請求件數超過處理件數額度，機關可請廠商提出服務費用報價或於下單前約定超出之資安事件處理(鑑識)處理費用。

（2）資安事件處理工作範圍包括：

A、廠商必須進行受駭原因分析與影響範圍之確認，並協助機關將造成資安事件的漏洞關閉，以避免進一步擴散。

B、檢測疑似被入侵之主機系統，針對系統資訊、日誌檔及惡意程式進行蒐集，日誌檢視以一年為原則(含線上與離線日誌)。

C、針對蒐集的資訊進行證物保存、磁碟映像檔分析、惡意程式分析及網路流量分析。以動態或靜態方法分析惡意程式功能，瞭解駭客入侵之主要目的。

D、將磁碟映像檔、惡意程式及網路封包等分析結果加以彙整進行關聯分析，以研判駭客入侵手法、入侵時間、影響範圍及威脅程度等。

4、資安威脅預警

（1）資安威脅預警服務範圍為廠商發現及蒐集國內外資安組織之資安威脅情資，至少包括：

A、資安聯防情資：行政院資通安全處不定時提供之惡意中繼站清單、高危險惡意特徵情資及其他情資通報。

B、病毒資訊警訊：如趨勢科技、Symantec 等防毒廠商中級以上病毒警訊。

C、系統弱點公告：如 NCCST、Microsoft、SecurityFocus 及各國 CERT 等國內外資安組織公告。

D、網頁攻擊資訊：如 Zone-H、OWASP 資安組織公告等。

E、新聞事件：如 CNN、Google 及 Yahoo 等資安新聞。

F、廠商發現之威脅：如 Zero-Day 事件。

（2）國內外資安威脅發表後 3 個工作日，整理相關訊息於客戶服務網站，並以電子郵件通知機關，提供資安威脅預警通報服務，內容包含資訊安全威脅類型、說明、可能造成之影響、

各大原廠發布的最新修正檔、新發現資訊安全漏洞與補救措施、資訊安全事件報導、漏洞分析、修補方式或對策。

（3）資安威脅預警通報後 2 個工作日，廠商通知機關監控服務範圍設置防禦措施，並提供資安威脅預警處理紀錄予機關。預警處理包含：

A、提供防火牆，IPS/IDS 等偵測規則諮詢。

B、提供如中繼站清單、高危險惡意特徵之阻擋與規則更新資訊等。

C、提醒更新系統安全或防毒軟體修正檔，或漏洞修補等。

5、計價估算

項目	單位	服務所需人天	SOC 監控服務-低流量服務總金額
SOC 監控環境部署 監控服務 資安事件處理 資安威脅預警	**一年服務**	365	(365*人天費率)

註：一年服務為全年全天候監控(365 天 x24 小時)，服務所需人天數為 365 天，每日以 24 小時計。

（二）SOC 監控服務人員資格

參與 SOC 監控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。SOC 監控服務人員，應具備必要之各類資訊網路、系統技能條件說明如下：

1、網路管理：接受過 CCNA (Cisco Certified Network Associate) 或其他類似網路管理相關課程訓練證明。

2、封包分析：接受過 NSPA (Network Security Packet Analysis)或其他類似相關課程訓練證明。

3、系統管理：接受過 MCSE (Microsoft Certified Solutions Expert)、LPIC (Linux Professional Institute Certification)、RHCE (Red Hat Certified Engineer)或其他類似相關課程訓練證明(以上訓練證明擇一)。

為順利於履約前驗證服務人員資格條件，廠商應就上述資格條件先行

確認合格，再檢附成員姓名、訓練證書、專業證照等影本報請適用機關同意後始得服務。

服務人員須年滿 18 歲，身體健康、無法定傳染病，且具有中華民國國籍，不得為外籍勞工或大陸來台人士。於履約期間內，廠商團隊成員不得同時受僱於大陸地區，或有於大陸地區執業、工作等情形。

（三）廠商應配合事項及交付項目

1、SOC 監控環境部署建議報告。

2、SOC 監控服務月報。

3、SOC 監控服務季報。

4、SOC 監控服務年報。

5、資安事件處理報告。

6、資安威脅預警報告。

7、配合適用機關辦理至少一次說明會議。

（四）文件報告基本要求

1、SOC 監控設備部署建議報告

如服務說明要求。

2、SOC 監控服務報告(月報、季報、年報)

（1）摘要說明。

（2）執行情形如服務說明要求。

（3）執行建議針對各項結果，提出改善建議。

（4）結論。

3、資安事件處理報告

如服務說明要求。

4、資安威脅預警報告

如服務說明要求。

（五）適用機關配合事項

機關須提供適當環境配合 SOC 監控環境部署。

第 2 項：SOC 監控服務-中流量

SOC 監控服務提供防毒軟體、網路防火牆、應用程式防火牆、APT 防護機制、電子郵件過濾機制及 IDS/IPS 等資安事件監控及分析統計報表。透過監控及分析，可將防毒軟體、網路防火牆、應用程式防火牆、APT 防護機制、電子郵件過濾機制及 IDS/IPS 等所產生的資安日誌，以系統化方式進行收集、關聯性分析後，定期產生報表，提供給客戶作為資訊安全的管理依據。

受監控的網路整體處理效能可達 2300 EPS(Event Per Second)，為分析日誌種類，設備數量或以網路流量推算所得。機關訂購前可根據日誌種類 EPS 參考表，加總機關內擁有的資安設備 EPS，計算監控所需要的 EPS 總量。

日誌種類參考表：

日誌種類	型式	EPS
網路設備(路由器)		250
資安設備(Firewall 防火牆)	低階	300
	高階	500
資安設備(IDS)	低階	150
	高階	450
資安設備(IPS)	低階	250
	中階	300
	高階	500
資安設備(WAF 防火牆)	低階	300
	中階	400
	高階	1500
個人防毒(防毒伺服器，防毒閘道器)		150
網站主機	低階	300
	高階	500
代理伺服器		250
郵件伺服器		200
郵件管理過濾器		150
目錄伺服器		150
檔案伺服器		150

日誌種類	型式	EPS
資料庫伺服器		500
DNS 伺服器	低階	150
	高階	250

（一）服務說明

1、SOC 監控環境部署

（1）廠商應於機關訂購單通知之次工作日起算 30 個日曆天內，勘查機關現有網路環境與需求，提出部署建議報告，並部署監控必要之遠端偵測器(日誌收集或 SIEM 等事件收集器)，所部署之設備不得影響現有各項安全設備之正常運作。部署工作應包括事件收集設備安裝、網段部署、設定、系統調校與重要資安事件 Rule 導入等工作。

（2）廠商發現事件收集設備故障，必須於 24 小時以內修復完成或調換同等級以上之相容設備。

（3）全年故障次數、總時間與搶救恢復時限作為指標，一般全年故障次數不可超過 5 次，故障總時間不可超過 78 小時，每次須於 24 小時內完成修復。

（4）若部署設備之實地場所有多處，最多以 5 處為限，超過額度部分，機關可請廠商提出服務費用報價或於下單前約定超出之服務費用。

（5）若機關有調整監控設備部署之需求，最多全年不得超過 10 次，超過額度部分，機關可請廠商提出服務費用報價或於下單前約定超出之服務費用。

2、監控服務

（1）廠商應遵循行政院國家資通安全會報技術服務中心制定之「政府領域聯防監控作業規範」，通過連通測試作業，並協助機關回傳資安監控情資至指定之聯防監控平台。

（2）廠商所提供之監控服務系統可從被監控端取得不同來源的日誌，經後送回 SOC 進行交叉比對後，可歸納出疑似資安事件或惡意軟體行為，能從警示系統產生工單、或者事件單

由專業資安人員判斷是否為資安事件。

（3）監控事件經監控中心判斷為資安事件時，應即以適當方式(以電話、傳真、手機簡訊、電子郵件等)通知機關資安連絡人，俾其依「資通安全事件通報及應變辦法」之規定於知悉資安事件 1 小時內進行資安事件通報。

（4）廠商應定期提供月報、季報予機關，俾其依「資通安全責任等級分級辦法」之相關規定提交監控管理資料。報告需提供以下內容：

A、事件通知或警訊發布統計

發生事件編號、事件名稱、事件處理結果。

持續追蹤的資安事件列表。

造成受監控設備停止或受影響時間。

受影響 IP 列表。

B、監控與警示系統監控情形

事件工單處理狀態與數量。

機關內員工連接中繼站(IP、DNS)數量。

惡意軟體攻擊類型說明與數量。

受攻擊服務統計圖表。

C、資安事件處理說明

處理紀錄說明。

提供防禦措施說明。

D、資安威脅預警情形

資安威脅預警公告。

資安威脅預警建議。

資安威脅預警諮詢。

E、評估建議改善項目

資安監控服務狀況報告，月報得以電子郵件或客戶服務網站等方式獲得，季報則須到府進行提報。

3、資安事件處理

（1）若發生資安事件，機關可向廠商提出事件處理服務需求，處理件數共 7 件，若請求件數超過處理件數額度，機關可請廠

商提出服務費用報價或於下單前約定超出之資安事件處理(鑑識)處理費用。

（2）資安事件處理工作範圍：

A、廠商必須進行受駭之原因分析與影響範圍之確認，並協助機關將資安事件造成的漏洞關閉，以避免進一步的擴散。

B、檢測疑似被入侵之主機系統，針對系統資訊、日誌檔及惡意程式進行蒐集，日誌檢視以一年為原則(含線上與離線日誌)。

C、針對蒐集的資訊進行證物保存、磁碟映像檔分析、惡意程式分析及網路流量分析。以動態或靜態方法分析惡意程式功能，瞭解駭客入侵之主要目的。

D、將磁碟映像檔、惡意程式及網路封包等分析結果加以彙整進行關聯分析，以研判駭客入侵手法、入侵時間、影響範圍及威脅程度等。

4、資安威脅預警

（1）資安威脅預警服務範圍，為廠商發現及蒐集國內外資安組織之資安威脅情資，至少包含：

A、資安聯防情資：行政院資通安全處不定時提供之惡意中繼站清單、高危險惡意特徵情資及其他情資通報。

B、病毒資訊警訊：如趨勢科技及 Symantec 等防毒廠商中級以上病毒警訊。

C、系統弱點公告：如 NCCST、Microsoft、SecurityFocus、各國 CERT 等國內外資安組織公告。

D、網頁攻擊資訊：如 Zone-H、OWASP 資安組織公告等。

E、新聞事件：如 CNN、Google 及 Yahoo 等資安新聞。

F、廠商發現之威脅：如 Zero-Day 事件。

（2）國內外資訊安全威脅發表後 3 個工作日，整理相關訊息於客戶服務網站，並以電子郵件通知機關，提供資安威脅預警通

報服務，內容包含：資訊安全威脅類型、說明、可能造成之影響、各大原廠發布的最新修正檔、新發現資訊安全漏洞與補救措施、資訊安全事件報導、漏洞分析、修補方式或對策。

（3）資安威脅預警通報後 2 個工作日，廠商通知機關監控服務範圍設置防禦措施，並提供資安威脅預警處理紀錄予機關，預警處理包含：

A、提供防火牆，IPS/IDS 等偵測規則諮詢。

B、提供如中繼站清單、高危險惡意特徵之阻擋與規則更新資訊等。

C、提醒更新系統安全或防毒軟體修正檔，或漏洞修補等。

5、計價估算

項目	單位	服務所需人天	SOC 監控服務- 中流量服務總金額
SOC 監控環境部署 監控服務 資安事件處理 資安威脅預警	**一年服務**	365	(365*人天費率)

註: 一年服務為全年全天候監控(365 天 x24 小時)，服務所需人天數為 365 天，每日以 24 小時計。

（二）SOC 監控服務人員資格

參與 SOC 監控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。SOC 監控服務人員，應具備必要之各類資訊網路、系統技能說明如下：

1、網路管理：接受過 CCNA (Cisco Certified Network Associate)或其他類似網路管理相關課程訓練證明。

2、封包分析：接受過 NSPA (Network Security Packet Analysis)或其他類似相關課程訓練證明。

3、系統管理：接受過 MCSE (Microsoft Certified Solutions Expert)、LPIC (Linux Professional Institute Certification)、RHCE (Red Hat Certified Engineer)或其他類似相關課程訓練證明(以上訓練證明擇

一)。

為順利於履約前驗證服務人員資格條件，廠商應就上述資格條件先行確認合格，再檢附成員姓名、訓練證書、專業證照等影本報請適用機關審核同意後始得服務。

服務人員須年滿 18 歲，身體健康、無法定傳染病，且具有中華民國國籍，不得為外籍勞工或大陸來台人士。於履約期間內，廠商團隊成員不得同時受僱於大陸地區，或有於大陸地區執業、工作等情形。

（三）廠商應配合事項及交付項目

1、SOC 監控環境部署建議報告。

2、SOC 監控服務月報。

3、SOC 監控服務季報。

4、SOC 監控服務年報。

5、資安事件處理報告。

6、資安威脅預警報告。

7、配合適用機關辦理至少一次說明會議。

（四）文件報告基本要求

1、SOC 監控設備部署建議報告

如服務說明要求。

2、SOC 監控服務報告(月報、季報、年報)

（1）摘要說明。

（2）執行情形

如服務說明要求。

（3）執行建議

針對各項結果，提出改善建議。

（4）結論

3、資安事件處理報告

如服務說明要求。

4、資安威脅預警報告

如服務說明要求。

（五）適用機關配合事項

機關須提供適當環境配合 SOC 監控環境部署。

第 3 項：SOC 監控服務-高流量

SOC 監控服務提供防毒軟體、網路防火牆、應用程式防火牆、APT 防護機制、電子郵件過濾機制及 IDS/IPS 等資安事件監控及分析統計報表。透過監控及分析，可將防毒軟體、網路防火牆、應用程式防火牆、APT 防護機制、電子郵件過濾機制及 IDS/IPS 等所產生的資安日誌，以系統化方式進行收集、關聯性分析後，定期產生報表，提供給客戶作為資訊安全的管理依據。

受監控的網路整體處理效能可達 4900 EPS(Event Per Second)，為分析日誌種類，設備數量或以網路流量推算所得。機關訂購前可根據日誌種類 EPS 參考表，加總機關內擁有的資安設備 EPS，計算監控所需要的 EPS 總量。

日誌種類參考表：

日誌種類	型式	EPS
網路設備(路由器)		250
資安設備(Firewall 防火牆)	低階	300
	高階	500
資安設備(IDS)	低階	150
	高階	450
資安設備(IPS)	低階	250
	中階	300
	高階	500
資安設備(WAF 防火牆)	低階	300
	中階	400
	高階	1500
個人防毒(防毒伺服器，防毒閘道器)		150
網站主機	低階	300
	高階	500
代理伺服器		250
郵件伺服器		200
郵件管理過濾器		150
目錄伺服器		150
檔案伺服器		150

日誌種類	型式	EPS
資料庫伺服器		500
DNS 伺服器	低階	150
	高階	250

（一）服務說明

1、SOC 監控環境部署

（1）廠商應於機關訂購單通知之次工作日起算 30 個日曆天內，勘查機關現有網路環境與需求，提出部署建議報告，並部署監控必要之遠端偵測器(日誌收集或 SIEM 等事件收集器)，所部署之設備不得影響現有各項安全設備之正常運作。部署工作應包括事件收集設備安裝、網段部署、設定、系統調校與重要資安事件 Rule 導入等工作。

（2）廠商發現事件收集設備故障，必須於 24 小時以內修復完成或調換同等級以上之相容設備。

（3）全年故障次數、總時間與搶救恢復時限作為指標，一般全年故障次數不可超過 5 次，故障總時間不可超過 52 小時，每次須於 24 小時內完成修復。

（4）若部署設備之實地場所有多處，最多以 7 處為限，超過額度部分，機關可請廠商提出服務費用報價或於下單前約定超出之服務費用。

（5）若機關有調整監控設備部署之需求，最多全年不得超過 12 次，超過額度部分，機關可請廠商提出服務費用報價或於下單前約定超出之服務費用。

2、監控服務

（1）廠商應遵循行政院國家資通安全會報技術服務中心制定之「政府領域聯防監控作業規範」，通過連通測試作業，並協助機關回傳資安監控情資至指定之聯防監控平台。

（2）廠商所提供之監控服務系統可從被監控端取得不同來源的日誌，經後送回 SOC 進行交叉比對後，可歸納出疑似資安事件或惡意軟體行為，能從警示系統產生工單、或者事件單

由專業資安人員判斷是否為資安事件。

（3）監控事件經監控中心判斷為資安事件時，應即以適當方式(以電話、傳真、手機簡訊、電子郵件等)通知機關資安連絡人，俾其依「資通安全事件通報及應變辦法」之規定於知悉資安事件 1 小時內進行資安事件通報。

（4）廠商應定期提供月報、季報予機關，俾其依「資通安全責任等級分級辦法」之相關規定提交監控管理資料。報告需提供以下內容：

A、事件通知或警訊發布統計

發生事件編號、事件名稱、事件處理結果。

持續追蹤的資安事件列表。

造成受監控設備停止或受影響時間。

受影響 IP 列表。

B、監控與警示系統監控情形

事件工單處理狀態與數量。

機關內員工連接中繼站(IP、DNS)數量。

惡意軟體攻擊類型說明與數量。

受攻擊服務統計圖表。

C、資安事件處理說明：

處理紀錄說明。

提供防禦措施說明。

D、資安威脅預警情形：

資安威脅預警公告。

資安威脅預警建議。

資安威脅預警諮詢。

E、評估建議改善項目：

資安監控服務狀況報告，月報得以電子郵件或客戶服務網站等方式獲得，季報則須到府進行提報。

3、資安事件處理

（1）若發生資安事件，機關可向廠商提出事件處理服務需求，處理件數共 15 件，若請求件數超過處理件數額度，機關

可請廠商提出服務費用報價或於下單前約定超出之資安事件處理(鑑識)處理費用。

（2）資安事件處理工作範圍包括：

A、廠商必須進行受駭之原因分析和影響範圍之確認，並協助機關將資安事件造成的漏洞關閉，以避免進一步的擴散。

B、檢測疑似被入侵之主機系統，針對系統資訊、日誌檔及惡意程式進行蒐集，日誌檢視以一年為原則(含線上與離線日誌)。

C、針對蒐集的資訊進行證物保存、磁碟映像檔分析、惡意程式分析及網路流量分析。以動態或靜態方法分析惡意程式功能，瞭解駭客入侵之主要目的。

D、將磁碟映像檔、惡意程式及網路封包等分析結果加以彙整進行關聯分析，以研判駭客入侵手法、入侵時間、影響範圍及威脅程度等。

4、資安威脅預警

（1）資安威脅預警服務範圍，為廠商發現及蒐集國內外資安組織之資安威脅情資，至少包含：

A、資安聯防情資：行政院資通安全處不定時提供之惡意中繼站清單、高危險惡意特徵情資及其他情資通報。

B、病毒資訊警訊：如趨勢科技及 Symantec 等防毒廠商中級以上病毒警訊。

C、系統弱點公告：如 NCCST、Microsoft、SecurityFocus、各國 CERT 等國內外資安組織公告。

D、網頁攻擊資訊：如 Zone-H、OWASP 資安組織公告等。

E、新聞事件：如 CNN、Google 及 Yahoo 等資安新聞。

F、廠商發現之威脅：如 Zero-Day 事件。

（2）國內外資訊安全威脅發表後 3 個工作日，整理相關訊息於客戶服務網站，並以電子郵件通知機關，提供資安威脅預警通報服務，內容包含資訊安全威脅類型、說明、可能造成之影響、各大原廠發布的最新修正檔、新發現資訊安全漏洞與

補救措施、資訊安全事件報導、漏洞分析、修補方式或對策。

（3）資安威脅預警通報後 2 個工作日，廠商通知機關監控服務範圍設置防禦措施，並提供資安威脅預警處理紀錄予機關。預警處理包含：

A、提供防火牆，IPS/IDS 等偵測規則諮詢。

B、提供如中繼站清單、高危險惡意特徵之阻擋與規則更新資訊等。

C、提醒更新系統安全或防毒軟體修正檔，或漏洞修補等。

5、計價估算

項目	單位	服務所需人天	SOC 監控服務- 高流量服務總金額
SOC 監控環境部署 監控服務 資安事件處理 資安威脅預警	一年服務	365	(365*人天費率)

註: 一年服務為全年全天候監控(365 天 x24 小時)，服務所需人天數為 365 天，每日以 24 小時計。

（二）SOC 監控服務人員資格

參與 SOC 監控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。SOC 監控服務人員，應具備必要之各類資訊網路、系統技能說明如下:

1、網路管理：接受過 CCNA (Cisco Certified Network Associate)或其他類似網路管理相關課程訓練證明。

2、封包分析：接受過 NSPA (Network Security Packet Analysis)或其他類似相關課程訓練證明。

3、系統管理：接受過 MCSE (Microsoft Certified Solutions Expert)、LPIC (Linux Professional Institute Certification)、RHCE (Red Hat Certified Engineer)或其他類似相關課程訓練證明(以上訓練證明擇一)。

為順利於履約前驗證服務人員資格條件，廠商應就上述資格條件先行確認合格，再檢附成員姓名、訓練證書、專業證照報請適用機關審核

同意後始得服務。

服務人員須年滿 18 歲，身體健康、無法定傳染病，且具有中華民國國籍，不得為外籍勞工或大陸來台人士。於履約期間內，廠商團隊成員不得同時受僱於大陸地區，或有於大陸地區執業、工作等情形。

（三）廠商應配合事項及交付項目

1、SOC 監控設備部署建議報告。

2、SOC 監控服務月報。

3、SOC 監控服務季報。

4、SOC 監控服務年報。

5、資安事件處理報告。

6、資安威脅預警報告。

7、配合適用機關辦理至少一次說明會議。

（四）文件報告基本要求

1、SOC 監控環境部署建議報告

如服務說明要求。

2、SOC 監控服務報告(月報、季報、年報)

（1）摘要說明

（2）執行情形

如服務說明要求。

（3）執行建議

針對各項結果，提出改善建議。

（4）結論

3、資安事件處理報告

如服務說明要求。

4、資安威脅預警報告

如服務說明要求。

（五）適用機關配合事項

機關須提供適當環境配合 SOC 監控環境部署。

三、第 3 組弱點掃描服務

訂購後半年內，提供適用機關 2 次弱點掃描服務(初掃與複掃)，針對主機系統或 Web 網頁進行安全弱點掃描，可評估掃描標的物是否存在安全弱點，同時提供給客戶相關掃描結果，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）服務說明

1、掃描內容:弱點掃描分為主機系統弱點掃描與 Web 網頁弱點掃描。

（1）主機系統弱點掃描

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：

A、作業系統未修正的漏洞掃描

B、常用應用程式漏洞掃描

C、網路服務程式掃描

D、木馬、後門程式掃描

E、帳號密碼破解測試

F、系統之不安全與錯誤設定檢測

G、網路通訊埠掃描

（2）Web 網頁弱點掃描

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 OWASP TOP 10 2017 項目：(官方網站如有公布更新資訊內容，請廠商以最新內容檢測)

A、A1-Injection

B、A2-Broken Authentication

C、A3- Sensitive Data Exposure

D、A4- XML External Entities (XXE)

E、A5- Broken Access Control

F、A6- Security Misconfiguration

G、A7- Cross-Site Scripting (XSS)

H、A8- Insecure Deserialization

Ⅰ、A9-Using Components with Known Vulnerabilities

Ｊ、A10- Insufficient Logging&Monitoring

2、掃描方式

掃描工具需取得授權使用的商用軟體，於非公務時段或與機關協調取得適當時間進行掃描作業。

3、分析報告

掃描作業後 1 個月內，根據掃描結果，將所發現之弱點與過程詳細記錄，並對結果進行分析，提出相關建議與掃描報告，以提供作為弱點修補之參考。

4、計價估算

項目	單位	服務所需人天	採購數量(例)	採購數量所需人天(服務所需人天*採購數量)	單項服務金額(採購數量所需人天*人天費率)
主機系統弱點掃描(VA)-到場服務 **(最低採購數量不得低於 15 IP)**	**IP**	**0.35**	0	0	
主機系統弱點掃描(VA)-遠端服務 **(最低採購數量不得低於 10 IP)**	**IP**	**0.3**	100	30	
WEB 網頁弱點掃描(WebVA)-到場服務	**URL**	**3**	0	0	
WEB 網頁弱點掃描(WebVA)-遠端服務	**URL**	**2**	10	20	
弱點掃描服務總金額					

註:各項服務所需人天數為工作日，每日以 8 個工作小時計。(所需人天為該項服務從規劃到完成之人天數，非實際到場人天)

（二）弱點掃描服務人員資格

參與弱點掃描服務人員應具備以下所列舉之技能，以確保服務水準。弱點掃描服務人員，應具備必要之各類資訊網路、系統技能，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證明證明(以上訓練證明擇一)。

為順利於履約前驗證服務人員資格條件，廠商應就上述資格條件先行確認合格，再檢附成員姓名、訓練證書、專業證照等影本報請適用機關審核同意後始得服務。

服務人員須年滿 18 歲，身體健康、無法定傳染病，且具有中華民國國籍，不得為外籍勞工或大陸來台人士。於履約期間內，廠商團隊成員不得同時受僱於大陸地區，或有於大陸地區執業、工作等情形。

（三）廠商應配合事項及交付項目

1、弱點掃描服務中文報告 (初掃與複掃均需提供)。

2、配合適用機關初掃與複掃各辦理至少一次說明會議。

（四）文件報告基本要求

1、執行結果摘要說明。

2、執行計畫

執行期間/執行項目/執行範圍/專案成員。

3、執行情形

A、整體結果統計說明。

B、檢測時間、檢測方式、檢測工具說明。

C、弱點摘要及分析說明。

D、安全強化建議。

4、結果建議

針對各項結果，提出改善建議。

5、結論

（五）適用機關配合事項

掃描與複掃作業時間與機關協調取得適當時間進行。

四、第 4 組滲透測試服務

訂購後半年內，提供適用機關 2 次滲透測試服務(初測與複測)，滲透測試係透過模擬駭客的攻擊方式，對目標主機或網路服務進行安全強度的測試，以找出可能的資安漏洞,並提出改善建議,並於協助修正資安漏洞後提供複測，以確認已經完成修正。

（一）服務說明

廠商針對機關之伺服器／主機作業系統、應用軟體、網路服務、可直接使用 RJ45 進行連線(配有 IP)之物聯網設備如：門禁設備、網路印表機、網路攝影機(IPCAM)、無線 AP/無線路由器或環控系統(監控溫度或濕度之機房環控系統的伺服器主機)等安全弱點與漏洞，進行滲透或穿透跳躍主機之入侵測試，設法取得未經授權之存取權限，並測試內部資訊是否有遭受不當揭露、竄改或竊取之可能性。

1、資料蒐集

對受測目標進行資料蒐集與資訊分析(如：嘗試至受測物聯網設備官方網站或透過網路資源取得韌體、使用的通訊方法，以及對應之弱點資訊，若查無公開可下載之韌體或該韌體具保護機制，則蒐集該設備已知弱點資料)，將取得之相關資訊做為執行滲透測試決策。

2、分析報告

測試作業後 1 個月內，根據測試結果，將所發現之弱點與過程詳細記錄(過程與結果需有佐證畫面)，並對結果進行確認，降低誤判問題(false positive、false negative)，提出相關建議與測試報告。

3、風險管理

在滲透測試執行期前，需提出對受測目標進行備份建議，避免發生非預期資料損毀或遺失等情形。

在滲透測試執行期間，執行具侵入性質的檢測作業皆需與機關進行確認，並於雙方議定之適當時間且具備適當應變措施與風險評估後，才進行相關檢測作業。

4、測試內容

測試類型	測試類別	測試項目
作業系統	遠端服務	至少包含遠端服務套件弱點測試等項目
	本機服務	在已取得系統控制權限的條件下,可執行至少包含本機服務套件弱點測試等項目
網站服務	設定管理	至少包含應用程式設定測試、檔案類型處理測試、網站檔案爬行測試、後端管理介面測試及 HTTP 協定測試等項目
	使用者認證	至少包含機敏資料是否透過加密通道進行傳送及使用者帳號列舉測試等項目
	連線管理	至少包含 Session 管理測試、Cookie 屬性測試、Session 資料更新測試、Session 變數傳遞測試及 CSRF 測試等項目
	使用者授權	至少包含目錄跨越測試、網站授權機制測試及權限控管機制測試等項目
	邏輯漏洞	至少包含網站功能測試、網站功能設計缺失測試及附件上傳測試等項目
	輸入驗證(1)	至少包含 XSS 漏洞測試、SQL Injection 測試、LDAP Injection 測試、XML Injection 測試、SSI Injection 測試、XPath Injection 測試及 Code Injection 測試等項目
	輸入驗證(2)	至少包含 XSS 漏洞測試、SQL Injection 測試、OS Commanding 測試及偽造 HTTP 協定測試等項目
	Web Service	至少包含 WSDL 測試、XML 架構測試、XML 內容測試及 XML 參數傳遞測試等項目
	Ajax	至少包含 Ajax 弱點測試等項目，如輸入驗證缺失、權限控管及套件弱點等測試項目
應用程式	電子郵件服務套件	至少包含 SMTP、POP3 及 IMAP 等常見對外郵件服務之弱點測試,如設定缺失、權限控管及套件弱點等測試項目

測試類型	測試類別	測試項目
	網站服務套件	包含常見 WEB 套件弱點測試，如設定缺失、權限控管及套件弱點等測試項目
	檔案傳檔服務套件	至少包含 FTP、NETBIOS 及 NFS 等常見檔案傳輸服務之弱點測試，如設定缺失、權限控管及套件弱點等測試項目
	遠端連線服務套件	至少包含 SSH、TELNET、VNC 及 RDP 等常見遠端連線服務之弱點測試，如設定缺失、權限控管及套件弱點等測試項目
	網路服務套件	至少包含 DNS、PROXY 及 SNMP 等常見網路服務之弱點測試，如設定缺失、權限控管及套件弱點等測試項目
	其它	包含 Firewall、IDS/IPS、Database、LDAP、SMB、LPD、IPP、Jetdirect 及 RTSP 等常見應用程式或網路套件之弱點檢測項目
密碼破解	密碼強度測試	至少包含 WEB、FTP、SSH、TELNET、SMTP、POP3、IMAP、SNMP、NetBIOS、RDP、VNC 及 Database 等常見對外服務之密碼字典檔測試
無線服務	無線服務弱點測試	到場服務的條件下，包含無線服務套件弱點測試與 WiFi 密碼字典檔測試等項目

5、計價估算(A)

項目	單位	服務所需人天	採購數量(例)	採購數量所需人天(服務所需人天*採購數量)	單項服務金額(採購數量所需人天*人天費率)
滲透測試(PT)-到場服務	**URL 或 IP**	**16**	1	16	
滲透測試(PT)-遠端服務	**URL 或 IP**	**15**	100	1500	
滲透測試服務總金額					

註:各項服務所需人天數為工作日，每日以 8 個工作小時計。(所需人天為該項服務從規劃到完成之人天數，非實際到場人天)

（二）滲透測試服務人員資格

參與滲透測試服務人員應具備以下所列舉之技能，以確保服務水準。

滲透測試服務人員,應具備必要之各類資訊網路、系統技能說明如下：

1、滲透測試工具使用：接受過 CEH(Certified Ethical Hacker)、EC-Council CertifiedSecurity Analyst (ECSA)或其他類似相關課程訓練(以上訓練證明擇一)。

2、滲透測試服務：接受過 GPEN (GIAC Certified Penetration Testers)、**GWAPT (GIAC Web Application Penetration Tester)**或其他類似相關課程訓練證明(以上訓練證明擇一)。

為順利於履約前驗證服務人員資格條件，廠商應就上述資格條件先行確認合格，再檢附成員姓名、訓練證書、專業證照等影本報請適用機關審核同意後始得服務。

服務人員需年滿 18 歲以上，身體健康無法定傳染病，且具有中華民國國籍，不得為外籍勞工或大陸來台人士，於履約期間不得同時於大陸地區工作。

（三）廠商應配合事項及交付項目

1、滲透測試服務報告。

2、配合適用機關初測與複測各辦理至少一次說明會議。

（四）文件報告基本要求(初測與複測均需提供)

1、執行結果摘要說明。

（1）受測目標風險等級與數量列表(依受測目標為序，表列包含之所有風險等級及其漏洞數量)

（2）受測目標風險漏洞名稱列表(依受測目標為序，表列包含之所有漏洞名稱、漏洞數量、風險等級及可能造成的風險)

（3）風險漏洞分布列表(依漏洞名稱為序，表列包含之漏洞數量、安全等級及受影響系統)

2、執行計畫

執行期間/執行項目/執行範圍/專案成員。

3、滲透測試執行結果

針對服務說明之所有測試項目提出測試結果(實際測試項目視受測主機或網站所提供的服務為主)，需說明詳細過程及內容(包括檢測目標/弱點名稱/問題 URL 或 IP/問題參數/測試語法/測試截圖等)，並說明可能造成的風險。

4、結果建議

針對執行結果提出改善建議。

5、結論

（五）適用機關配合事項

執行作業時間與機關協調取得適當時間進行，測試標的(IP/Domain)須在廠商服務執行前確認，服務執行期間不得再臨時變更。

五、第 5 組社交工程郵件測試服務

社交工程郵件檢測係透過電子郵件的方式提供受測單位瞭解社交工程的存在,並提高警覺性;同時受測單位可以根據測試結果瞭解可能發生安全缺口，藉以實施其內部教育訓練來補強，並作為資訊安全的管理依據。

（一）服務說明

1、服務項目

項次	項目	內容說明
1	受測對象與時間	訂購後 1 年內,提供購買單位電子郵件帳號 2 次的測試。各帳號進行 5 封社交工程郵件測試，採用可編輯文檔進行測試。
2	測試內容	郵件內容設計可涵蓋不同類型，例如：八卦、休閒、保健、財經、情色、新奇。各種類型提供至少 3 種不同的內容，以供隨機挑選進行測試。 記錄「開啟郵件」、「點閱連結」及「開啟附件」等受測者行為。
3	分析報告	整體結果統計圖表，不同類型/分組結果/排序統計表。 郵件派送時間表。 統計「開啟郵件」、「點閱連結」及「開啟附件」等受測者行為。 統計「郵件開啟率」與「郵件點閱率」等結果。 受測者開啟及點閱細部時間紀錄
4	諮詢服務	分析報告提出後 1 個月內提供 8x5 諮詢服務。

2、計價估算

項目	單位	服務所需人天	單項服務金額(服務所需人天*人天費率)
社交工程郵件檢測服務 (5 封信/每一帳號)	100 個帳號 (1~100)	10	
社交工程郵件檢測服務 (5 封信/每一帳號)	200 個帳號 (101~200)	11	

項目	單位	服務所需人天	單項服務金額(服務所需人天*人天費率)
社交工程郵件檢測服務 (5 封信/每一帳號)	500 個帳號 (201~500)	13	
社交工程郵件檢測服務 (5 封信/每一帳號)	1000 個帳號 (501~1000)	15	
社交工程郵件檢測服務總金額			

註 1: 訂購機關應依需檢測之帳號數量選擇合適之項目訂購，單一訂單不得同時包含 2(含)個以上不同單位之項目。如機關所需檢測之帳號數量超過 1,000 個以上，則無法利用本契約訂購，請自行依政府採購法相關規定辦理採購。

註 2: 各項服務單位所需人天數為工作日，每日以 8 個工作小時計。(所需人天為該項服務從規劃到完成之人天數，非實際到場人天)

（二）社交工程郵件測試服務人員資格

參與社交工程郵件測試服務人員，應具備以下所列舉之技能，以確保服務水準。社交工程郵件測試服務人員，應具備必要之各類資訊網路、系統技能，社交工程郵件測試服務：接受過 CEH(Certified Ethical Hacker)或其他類似相關課程訓練證明證明(以上訓練證明擇一)。

為順利於履約前驗證服務人員資格條件，廠商應就上述資格條件先行確認合格，再檢附成員姓名、訓練證書、專業證照等影本報請適用機關審核同意後始得服務。

服務人員須年滿 18 歲，身體健康、無法定傳染病，且具有中華民國國籍，不得為外籍勞工或大陸來台人士。於履約期間內，廠商團隊成員不得同時受僱於大陸地區，或有於大陸地區執業、工作等情形。

（三）廠商應配合事項及交付項目

1、社交工程郵件檢測服務報告。

2、配合適用機關辦理至少一次說明會議。

（四）文件報告基本要求

1、執行結果摘要說明

2、執行計畫

執行期間/執行項目/執行範圍/專案成員。

3、執行情形

（1）整體結果統計圖表。

（2）不同郵件類型測試的排序統計圖表。

（3）郵件派送時間表。

（4）統計開啟郵件/點閱連結/開啟附件等受測者行為與細部時間紀錄。

4、結果建議

針對各項結果，提出改善建議。

5、結論

（五）適用機關配合事項

執行作業時間與機關協調取得適當時間進行。

六、第 6 組防火牆服務

(一) 服務介紹

防火牆服務由立約服務供應商提供一部(Unified threat management, UTM)整合式威脅管理網路防火牆設備，協助政府機關建置該設備、更新防禦情資、維護防火牆設備並進行該設備資安政策管理，於網路閘道內提供：防火牆、VPN、入侵偵測與防禦(Intrusion Detection and Prevention，IDS/IPS)等資訊安全防護功能。另提供威脅告警與定期產生服務記錄報表，提供給政府機關作為網路資訊安全的管理依據。

政府機關可根據連外頻寬與網路處理流量需求，選擇所需要的 UTM 整合式威脅管理處理流量，包含：300Mbps、500Mbps 與 1Gbps 的不同等級之防火牆服務。

(二) 服務說明

1. 服務範圍

本項目服務標的為服務供應商所建置之網路防火牆設備，提供到場安裝服務與每年 4 次到場計劃性維護服務，日常服務作業將以遠端進行設定、防禦情資更新、系統更新、防火牆政策管理與設備維護等作業事項。

本服務自供應商完成網路防火牆設備建置後，提供 36 個月的維運服務，服務期滿供應商依契約條款第 17 條第 12 款約定處理。

2. 現行網路架構檢視

針對機關提供的網路架構圖進行安全性弱點檢視，依據網路架構安全設計、備援機制設計、網路設備管理、伺服器主機設備、網路存取管控、IP 網段配置、既有防火牆政策(Policy Rules)與開啟通訊埠位(Port)等資訊，檢視網路拓樸設計邏輯是否合宜、主機網路位置及通訊埠位是否適當及現有防護政策是否足夠等，用以設定新部署之網路防火牆政策。

3. 網路防火牆部署

立約商應於政府機關訂購單通知之次工作日起算 30 個日曆天內，檢視

政府機關現有網路架構與環境需求，提出網路防火牆設備部署建議報告，並與機關協調設備部署時間。部署工作應包含：網路防火牆設備安裝、網段部署設定、防火牆政策設定與系統調校及導入等工作。

若機關若有調整網路防火牆設備部署之需求，最多每年不得超過 1 次，並列入到場計劃性維護服務之中，機關若超過計劃性維護服務的部分，則不屬本服務範圍。

4. 網路防火牆維護

(1) 網路防火牆系統更新

依據防火牆設備原廠提供之新版系統軟體或韌體時程，與機關協調取得同意後進行設備系統更新之計劃性維護作業，並彙整記錄於每月服務報告。

(2) 防禦情資資料庫更新

立約商應於服務期間提供防火牆設備原廠的防禦情資使用授權，並依據設備原廠提供之最新防禦情資，定期更新防禦資料庫與設備設定，並彙整記錄於每月服務報告。

(3) 防火牆政策維護與管理

依據以下作業需求：

(a) 防火牆告警與威脅

(b) 機關使用的 IP 網段或伺服器主機 IP 位置等政策異動

(c) 機關的資安威脅預警

由立約商配合提出計劃性維護作業與進行防火牆政策更新與事件處理等作業，並彙整記錄於每月服務報告。

5. 防火牆告警與事件處理

立約商針對防火牆偵測的資安威脅與告警，進行事件處理或防火牆政策調整，並彙整記錄於每月服務報告。

6. 服務監控

提供每月網路防火牆服務監控報告，提供報告內容需包含以下項目：

(1) 網路流量統計記錄

(2) 網路資安威脅統計記錄

(3) 網路資安告警記錄

7. 服務要求

維護時間應於使用機關之辦公日（依行政院人事行政總處公布之上班日為準）每日上午 8 時 30 分至下午 5 時 30 分，不含例假日。

立約商應於接獲使用機關電話、傳真或書面維護作業需求後，於 2 小時以電話、Email、簡訊或其他書面方式回覆機關維護作業計劃，並於 1 個工作天以內完成系統更新與防火牆政策管理維護作業，如需配合機關日常業務進行，另外約定之維護計畫作業時間則不在此限制內。

全年設備故障次數、總時間與搶救時限要求，全年故障次數不可超過 5 次，故障總時間不可超過 104 小時，每次須於 1 個工作天內完成修復，唯計劃性維護作業不列入故障總時間及次數之中。

政府機關或廠商因天災或事變等不可抗力或不可歸責於契約當事人之事由，致未能依時履約者，得展延履約期限。

(三) 網路防火牆功能規格

本服務需具備防火牆政策管理、IDS/IPS 入侵偵測與防禦、IPSec VPN、SSL VPN、雲端沙箱、不當網頁過濾與應用程式控管及韌體更新服務等功能，部署設備需符合以下規格：

1. 防火牆防護能力需通過第三方資訊安全機構防火牆檢測認證如 NSS Labs 、 ISCA Labs 等。
2. 網路防火牆防護效能
   (1) UTM 整合式威脅管理處理流量可達 300 Mbps。
   (2) UTM 整合式威脅管理處理流量可達 500 Mbps。
   (3) UTM 整合式威脅管理處理流量可達 1Gbps。
3. VPN 效能
   (1) 300Mbps 之防火牆服務具備可同時建立 8 條 VPN 連線。
   (2) 500Mbps 之防火牆服務具備可同時建立 16 條 VPN 連線。
   (3) 1Gbps 之防火牆服務具備可同時建立 32 條 VPN 連線。
4. 網路防火牆具備 2 個以上 10/100/1000 自動偵測超高速乙太網路介面

的 WAN 埠介面，以及內建 4 個以上 10/100/1000 自動偵測超高速乙太網路介面，每埠可自行定義為 LAN 或 DMZ。

5. 支援多個不同安全網域（Security Zone），不同安全網域網段連通，需經防火牆政策（Firewall Policy）控管。
6. 支援 IDS/IPS 入侵偵測與防禦、Anti-Virus 網路防毒、Content Filtering 異常網頁過濾、與應用程式控管等資安防護功能。
7. 支援雲端智慧沙箱服務，協助模擬分析未知威脅，找出惡意程式與病毒特徵碼，提升零時差攻擊防禦能力減少資安攻擊事件。
8. 支援 IPSec VPN、SSL VPN，並符合 SHA-2（256-bit）標準之封包認證功能與 3DES 及 AES（256-bit）之加、解密演算標準。
9. 具備使用者認證功能（User Authentication）
10. 支援 IPv4 與 IPv6 網路路由功能。
11. 支援標準 19 吋機架安裝設計。
12. 符合 FCC Part 15（Class A）、CE EMC（Class A）及 BSMI 安規及電磁檢測標準。

(四) 廠商應配合事項及交付項目

1、網路防火牆部署建議報告

如服務說明要求。

2、每月提供網路防火牆服務報告，至少包含：

(1) 摘要說明

(2) 執行情形

如服務說明要求。

(3) 執行建議

針對各項服務內容，提出改善建議。

(4) 結論。

3、配合機關資安規定與稽核作業，提供相關協助。

(五) 服務人員資格

參與網路防火牆服務人員應具備資訊網路、防火牆系統之維護技能，以確保服務水準。需求技能條件說明如下：

1、網路管理：接受過 CCNA (Cisco Certified Network Associate) 或其他

類似網路管理相關課程訓練證明。

2、防火牆維護：具備防火牆設備原廠認證資格，以確保立約廠商具有網路資安與防火牆維護服務之能力。

為順利於履約前驗證服務人員資格條件，廠商應就上述資格條件先行確認合格，再檢附成員姓名、訓練證書、專業證照等影本報請適用機關同意後始得服務。

服務人員須年滿 18 歲，身體健康、無法定傳染病，且具有中華民國國籍，不得為外籍勞工或大陸來台人士。於履約期間內，廠商團隊成員不得同時受僱於大陸地區，或有於大陸地區執業、工作等情形。

(六) 機關配合事項

1. 機關須配合提供既有網路拓樸架構、使用 IP 網段、伺服器主機位置、VLAN 資訊及網路建置所必須資訊，並安排相關人員受訪確認機關網路環境。
2. 提供群組原則(Group Policy)、既有防火牆政策(Policy Rule)與開啟通訊埠(Port)的資訊，以供服務廠商設定建置防火牆政策維護。
3. 機關須提供適當環境配合安裝建置網路防火牆設備。
4. 機關如欲集中納管設備系統日誌，政府機關必須提供集中管理的日誌伺服器(Syslog Server)相關設定資訊，由服務廠商設定網路防火牆的日誌管理伺服器。