109 年共同供應契約資通安全服務品項採購規範

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測服務作業，提供受檢機關資安改善建議，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

項目		內容說明
1.網路架構檢視		針對網路架構圖進行安全性弱點檢視，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，應詳列發現事項之風險等級、風險說明與改善建議，於風險說明詳述問題範圍與可能之影響，並提出具體改善建議，以利機關後續修補與調整
2.網路惡意活動檢視(有線)	2.1 封包監聽與分析	1.針對有線網路適當位置架設封包側錄設備，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 2.發現異常連線之電腦或設備應確認使用狀況與用途 3.封包側錄至少以 6 小時為原則，以觀察是否有異常連線
	2.2 資安設備紀錄檔分析	1.檢視資安設備(如防毒軟體、網路防火牆、應用程式防火牆、APT 防禦措施、電子郵件過濾及 IDS/IPS 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 2.發現異常連線之電腦或設備應確認使用狀況與用途 3.資安設備紀錄檔分析以 1 個月或 100M byte 內的紀錄為原則
3.使用者端電腦惡意活動檢視	3.1 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
	3.2 使用者電腦更新檢視	1.檢視使用者電腦之 Microsoft 作業系統更新情形 2.檢視使用者電腦之應用程式之安全性更新情形(包括 Office 應用程式舉凡 word、powerpoint、Excel、Access…等)、Adobe Acrobat、Adobe flash player 及 Java 應用程式) 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)

項目		內容說明
		4.檢視使用者電腦防毒軟體安裝、更新及定期掃描結果之處理情形
4.伺服器主機惡意活動檢視	4.1 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
	4.2 伺服器主機更新檢視	1. 檢視伺服器之 Microsoft 作業系統更新情形 2. 伺服器之應用程式之安全性更新情形(包括 Office 應用程式（舉凡 word、powerpoint、Excel、Access…等）、Adobe Acrobat、Adobe flash player 及 Java 應用程式) 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 Server 2003、Office 2003) 4. 檢視伺服器是否使用不合宜之作業系統（如使用 Windows 7、Windows10） 5. 檢視伺服器主機防毒軟體安裝、更新及定期掃描結果之處理情形
5.目錄伺服器設定檢視		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 註：作為 AD server 之伺服器其 GCB 設定皆應檢視。
6.防火牆連線設定檢視		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)

項目	內容說明	
7. 政府組態基準(GCB)檢視	7.1 作業系統_使用者電腦組態設定檢視	1.針對使用者電腦組態設定檢視，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 2.使用者電腦組態設定檢視，如 Windows 7、Windows 8.1、Windows 10 等。
	7.2 作業系統_伺服器組態設定檢視	1.針對伺服器組態設定檢視，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 2.伺服器組態設定檢視，如 Windows Server 2008 R2、Windows Server 2012 R2、Windows Server 2016、RedHat Enterprise Linux 5 等。
	7.3 瀏覽器組態設定檢視	1.針對瀏覽器之組態設定檢視，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 2.瀏覽器之組態設定檢視，如 Internet Explorer 8、Internet Explorer 11、Google Chrome、Mozilla Firefox、Microsoft Edge 等。

項目	內容說明	
	7.4 網通設備組態設定檢視	1.針對網通設備組態設定檢視，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 2.針對網通設備組態設定檢視，如無線網路、Juniper Firewall、Fortinet Fortigate、Cisco Firewall 等。
	7.5 應用程式組態設定檢視	1.針對應用程式組態設定檢視，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 2.應用程式組態設定檢視，如 Exchange Server 2013、Microsoft IIS 8.5 等。

（二）計價方式：

項目	單位	各項服務單位所需人天	最低採購量	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)
1.1 網路架構檢視	網路架構	**2**	**1**	1	2	
2.1 網路惡意活動檢視(有線)_封包監聽與分析	側錄設備	**2**	**2**	2	4	

項目	單位	各項服務單位所需人天	最低採購量	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)
2.2 網路惡意活動檢視(有線)_資安設備紀錄檔分析	資安設備	**1**	**2**	2	2	
3.使用者端電腦惡意活動檢視	使用者電腦	**0.3**	**20**	20	6	
4.伺服器主機惡意活動檢視	伺服器	**0.3**	**5**	5	1.5	
5.目錄伺服器設定檢視	伺服器	**0.5**	**1**	1	0.5	
6.防火牆連線設定檢視	防火牆設備	**0.5**	**1**	1	0.5	
7.1 作業系統_使用者電腦組態設定檢視	使用者電腦	**0.3**	**10**	10	3	
7.2.作業系統_伺服器組態設定檢視	伺服器	**0.5**	**1**	1	0.5	
7.3 瀏覽器組態設定檢視	瀏覽器	**0.3**	**10**	10	3	
7.4.網通設備組態設定檢視	網通設備	**0.5**	**1**	1	0.5	
7.5.應用程式組態設定檢視	伺服器	**0.5**	**1**	1	0.5	
採購總人天						

註 1: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：

1. 本服務第 1 至 6 項為資安法之資安健診項目、第 7 項為政府組態基準(GCB)檢視，各服務細項分項採購，採購單位數量不得少於最低採購數量。
2. 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 1 名成員，以確保服務水準。

1. 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 1)。
   （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 1)。
2. 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。
3. 服務人員須年滿 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。

（五）廠商應交付文件與辦理項目：

1. 資安健診服務報告。
2. 配合機關辦理至少 1 次說明會議。

（六）交付文件基本要求：

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，應詳列發現事項之風險等級、風險說明與改善建議，於風險說明詳述問題範圍與可能之影響，並提出具體改善建議，以利機關後續修補與調整。

(2)網路惡意活動檢視(有線)

2.1.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應確認使用狀況與用途。

2.2.資安設備紀錄檔分析

依檢視之資安設備為序，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應確認使用狀況與用途。

(3)使用者端電腦惡意活動檢視

3.1 使用者電腦惡意程式或檔案檢視，依檢視之使用者電腦 IP 為序，分別說明檢視結果包括弱點說明、修補建議及發現之惡意程式檔名與改善建議。

3.2 使用者電腦之作業系統、Office 應用程式、防毒軟體、Adobe Acrobat 及 Adobe flash player 應用程式更新情形，

使用者電腦依檢視項目逐項詳列未更新之台數及比例數，並以附件方式詳列未更新之 IP、未更新筆數、未安裝更新編號等資訊。

(4)伺服器主機惡意活動檢視

4.1 伺服器主機惡意程式或檔案檢視，依檢視伺服器 IP 為序，分別說明檢視結果包括弱點說明、修補建議及發現之惡意程式檔名與改善建議。

4.2 伺服器主機之作業系統、Office 應用程式、防毒軟體、Adobe Acrobat 及 Adobe flash player 應用程式更新情形，分別依檢視項目逐項詳列未更新之台數及比例數，並以附件方式詳列未更新之 IP、未更新筆數、未安裝更新編號等資訊。

(5)目錄伺服器設定檢視

A. 目錄伺服器政府組態基準(GCB)整體摘要報告，項目總數、符合項目總數、不符合項目總數及例外管理之情形說明。

B. 詳列各項檢視設備之 IP、項目名稱、類別、版本、GCB 規定值、實際檢視結果。

C. 對於不符合項目，進一步了解機關不符合項目的原因，若為”例外管理”項目，註明依據機關例外管理設定值及檢視結果。

D. 對於未安裝之項目應標示為「未安裝」。

E. 其他的原因，了解後提出整體改善建議，以利機關後續改善。

(6)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，並表列說明應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。

(7)各項政府組態基準(GCB)檢視之結果：

A.政府組態基準檢視(GCB)整體摘要報告，項目總數、符合項目總數、不符合項目總數及例外管理之情形說明。

B.詳列各項檢視設備之 IP、項目名稱、類別、版本、GCB 規定值、實際檢視結果。

C.對於不符合項目，進一步了解機關不符合項目的原因，若為例外管理”項目，註明依據機關例外管理設定值及檢視結果。

D.對於未安裝之項目應標示為「未安裝」。

E.其他的原因，了解後提出整體改善建議，以利機關後續改善。

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)側錄封包資料(燒錄至光碟或其他媒體裝置)。

(2)服務紀錄檔(燒錄至光碟)

(3)發現惡意行為或惡意程式的過程紀錄與說明。

(4)使用者端電腦安全性未更新資訊。

(5)伺服器安全性未更新資訊。

（七）廠商應配合事項

1. 檢視服務之項目/數量與採購項目/數量相符。
2. 服務所需軟硬體設備由廠商提供。

（八）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，機關應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 資通安全威脅偵測管理(SOC)服務

第 1 項：資通安全威脅偵測管理(SOC)服務-低流量

資通安全威脅偵測管理(SOC)服務提供網通設備、資安防護措施(如防毒軟體、網路防火牆、應用程式防火牆、APT 防禦措施、電子郵件過濾及 IDS/IPS 等)、主機伺服器等資安事件監控、事件處理、資安威脅預警等服務。透過監控及分析，可將監控設備所產生的日誌，以系統化方式進行收集、關聯性分析後，提供給機關進行情資管理。

（一）監控服務處理效能：

1. 受監控設備之整體處理效能總達 900 EPS(Event Per Second)。
2. 監控 EPS 以日誌種類、設備數量推算所得，機關訂購前先參考機關過去 3 年之資安設備實際的 EPS 或表 1 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。
3. SOC 監控設備應納入資通安全責任等級分級辦法之資通安全防護措施(包括防毒軟體、網路防火牆、電子郵件過濾機制、IDS/IPS、應用程式防火牆及 APT 防禦措施等)，及機關之核心資通系統(含 AD)等資訊設備紀錄與服務/應用程式紀錄（應以上列整體處理效能 EPS 為原則）。

表 1 日誌種類 EPS 參考表

序號	日誌種類	型式	EPS
1	防毒軟體(防毒伺服器，防毒閘道器)		150
2	資安設備_網路防火牆	低階	300
		高階	500
3	郵件管理過濾機制		150
4	資安設備_IDS	低階	150
		高階	450
5	資安設備_IPS	低階	250
		中階	300
		高階	500
6	資安設備_應用程式防火牆(WAF)	低階	300
		中階	400

序號	日誌種類	型式	EPS
		高階	1500
7	資安設備_APT 防禦措施		150
8	網站主機	低階	300
		高階	500
9	網路設備(路由器)		250
10	代理伺服器		250
11	郵件伺服器		200
12	目錄伺服器		150
13	檔案伺服器		150
14	資料庫伺服器		500
15	DNS 伺服器	低階	150
		高階	250

（二）計價方式：

項目	單位	服務所需人天	SOC 監控服務-低流量服務總金額
1.SOC 監控環境部署 2.監控服務 3.資安事件處理 4.資安威脅預警	**1 年服務**	365	(365*人天費率)

註：1 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。

（三）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器安裝、網段部署、設定、系統調校與重要資安事件 Rule 導入等工作。

（2）Event 數量計算以事件收集器所收集的數量為基準；廠商應每季檢視受監控設備之 EPS 情形，檢視監控部署執行成效，適時提出部署調整建議。

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

（4）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，每次應於 24 小時內完成修復。

（5）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。

（6）若機關有調整監控設備部署之需求，全年不得超過 8 次，惟花東、離島、外島等偏遠地區，以 3 次異動為限，若超出次數，機關另需支付廠商差旅費；其他超出額度部分，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）廠商收集日誌後，透過資安監控機制進行整合與關聯，產生「資安監控單」(例如：Incident)。

（2）SOC 分析人員對「資安監控單」進行影響性評估，並產生「情資分析單」(例如:Ticket)，廠商應即時以適當方式(以電話、手機簡訊、電子郵件、網頁、傳真等)通知機關資安連絡人，俾利機關進行情資處理。

（3）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」，辦理下列事項：

A、連通測試：

廠商應通過資安聯防監控情資連通測試，尚未通過連通測試者，應填寫「資安情資回傳連通測試申請單」，提出申請並通過連通測試，確保廠商之情資回傳能力。

B、正式回傳作業辦理：

廠商應協助機關即時回傳資安監控服務之「資安監控單」

與「情資分析單」至指定之聯防監控平台；另依據監控設備之監控狀況，每月提交「監控設備狀況單」至指定之聯防監控平台。

C、聯防監控情資有效性檢核：

廠商應確保資安監控偵測與分析、資安情資回傳、資安監控情資內容品質之有效性。

D、廠商應確實協助公務機關配合政府領域聯防監控作業，除上述辦理事項外，亦應遵照機關其所屬領域主管機關訂定之作業規範，配合辦理 SOC 監控資訊回傳作業。

E、「資安監控單」、「情資分析單」及「監控設備狀況單」等表單格式應依行政院國家資通安全會報技術服務中心網站 https://www.nccst.nat.gov.tw/GSOC 公告之聯防監控資安情資回傳 STIX 格式規範。

（4）廠商應定期提交月報、季報、年報予機關，月報得以紙本文件或電子檔、網頁型式等方式提交，而季報、年報則應到府進行提報。

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、廠商必須進行受駭根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資料蒐集，日誌檢視以 1 年為原則(含線上與離線日誌)。

C、應針對蒐集的資料進行資料保存、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：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、Security Focus、各國 CERT(如 CISA(USCERT))及 MITRE 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，整理相關訊息通知機關，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。

（四）相關服務人員資格

1. 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 1)。

2. 資安事件處理人員，應具備必要之各類資訊網路、系統技能，接受過 CEH(Certified Ethical Hacker)或 ECIH(EC-Council Incident Handler)資安危機處理員認證或其他類似相關課程訓練證明(以上訓練證明擇 1)。

3. 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採購機關同意後始得服務。

4. 服務人員須年滿 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。

（五）廠商應交付文件及辦理項目：

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. 配合機關辦理至少 1 次說明會議。

（六）交付文件基本要求

1. SOC 監控設備部署建議報告

（1）提出工作計畫書，包括各項工作執行規劃、監控設備部署規劃、監控與警示作業之方式、通知機關資安連絡人之時機、內容及方式、資安事件處理之作業、資安威脅預警之作業

等。

（2）各項報告(月報、季報、年報)提交時間及內容。

2. SOC 監控服務月報

（1）監控與警示情形，除依規定時間通知機關與回傳指定之聯防監控平台外，亦應於機關之相關報告呈現。

A、當月「資安監控單」之產生數量及回傳數量等資訊。

B、當月「情資分析單」之產生數量、回傳數量及通知機關數量等資訊；另詳列「情資分析單」內容，包括表單編號、事件主旨、事件類別、觸發規則、來源 IP、目的 IP、事件描述、影響等級等與情資分析單有關之資訊。

C、當月之「監控設備狀況單」，呈現其監控設備運作情形。

D、監控情資之統計分析：（以下為基本要求，廠商或機關可再酌增項目）

a. 當月「情資分析單」之事件主旨、事件類別、觸發規則之統計分析。

b. 外部威脅連線 IP 清單，清整當月外部威脅連線 IP，可用於黑名單阻擋以利後續追蹤。

c. 其他。

E、機關之資安弱點及強化措施建議。

（2）資安事件處理

當月協助處理資安事件之彙整資訊及處理進度說明，詳細資安事件處理之報告以分件撰寫報告。

（3）資安威脅預警

A、當月資安威脅預警分類彙整，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。

B、建議設置防禦之措施及提供資安威脅預警諮詢服務紀錄。

（4）總結

3. SOC 監控服務季報

彙整當季之 SOC 監控、資安事件處理、資安威脅預警之重點，並且提出相關之統計、趨勢分析及強化防護建議，包括：

（1）監控與警示分析

A、當季統計分析：(以下為基本要求，廠商或機關可再酌增項目)

a. 當季「資安監控單」、「情資分析單」之統計，包括事件主旨、事件觸發規則及事件類別統計，說明近期機關遭受資安威脅趨勢。

b. 外部威脅連線 IP 清單，清整當季外部威脅連線 IP，可用於黑名單阻擋以利後續追蹤。

c. 其他

B、提供當季受監控設備之 EPS 資訊，檢視監控部署執行成效，適時提出部署調整建議。

C、綜整機關威脅趨勢、資安弱點及強化措施建議。

（2）資安事件處理

當季協助處理資安事件之彙整資訊及處理進度說明，詳細資安事件處理之報告以分件撰寫報告。

（3）資安威脅預警

A、資安威脅預警之分類與數量。

B、資安威脅重大預警重點摘要。

C、資安威脅預警趨勢分析。

D、機關可預防之建議。

（4）總結

4. SOC 監控服務年報

（1）監控與警示分析

A、年統計分析：(以下為基本要求，廠商或機關可再酌增項目)

a. 事件主旨、觸發規則、事件類別統計等，說明近 1 年機關遭受資安威脅趨勢。

b. 外部威脅連線 IP 清單，清整近 1 年外部威脅連線 IP，可用於黑名單阻擋以利後續追蹤。

c. 其他

B、綜整近 1 年機關之威脅趨勢、資安弱點及強化措施建議。

C、全年受監控資安設備之 EPS 統計，以供機關了解資安設備之處理效能，作為後續採購或監控部署之參考。

（2）資安事件處理

全年協助處理資安事件之彙整資訊及處理進度說明，詳細資安事件處理之報告以分件撰寫報告。

（3）資安威脅預警分析

A、 資安威脅預警整合分析。

B、 資安威脅重大預警重點摘要。

C、 資安威脅預警整合分析，並提出趨勢預測。

D、 機關可預防之建議。

（4）總結

5. 資安事件處理報告(分件撰寫報告)

針對各別資安事件之基本資訊，與資安事件處理等過程進行紀錄，並提出矯正預防措施建議，包括精進內部程序文件、強化安全防護、提升教育訓練等建議，以提升機關之防護能量。

（1）資安事件之基本資訊說明，包括事件編號、事件主旨、事件分級、發現時間、通報時間、受駭標的資料、事件類別、事件說明等。

（2）資安事件處理之根因調查及後續改善建議，包括資料蒐集、資料分析、根因分析、駭客入侵手法、入侵時間、影響範圍及後續追蹤改善項目等。

（七）機關配合事項

機關應提供適當環境配合 SOC 監控環境部署。

二、第 2 組 資通安全威脅偵測管理(SOC)服務

第 2 項：資通安全威脅偵測管理(SOC)服務-中流量

資通全威脅偵測管理(SOC)服務提供網通設備、資安防護措施(如防毒軟體、網路防火牆、應用程式防火牆、APT 防禦措施、電子郵件過濾及 IDS/IPS 等)、主機伺服器等資安事件監控、事件處理、資安威脅預警等服務。透過監控及分析，可將監控設備所產生的日誌，以系統化方式進行收集、關聯性分析後，提供給機關進行情資管理。

（一）監控服務處理效能：

1. 受監控設備之整體處理效能總達 2300 EPS(Event Per Second)。
2. 監控 EPS 以日誌種類、設備數量推算所得，機關訂購前先參考機關過去 3 年之資安設備實際的 EPS 或表 2 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。
3. SOC 監控設備應納入資通安全責任等級分級辦法之資通安全防護措施(包括防毒軟體、網路防火牆、電子郵件過濾機制、IDS/IPS、應用程式防火牆及 APT 防禦措施等)，及機關之核心資通系統(含 AD)等資訊設備紀錄與服務/應用程式紀錄（應以上列整體處理效能 EPS 為原則）。

表 2 日誌種類 EPS 參考表

序號	日誌種類	型式	EPS
1	防毒軟體(防毒伺服器，防毒閘道器)		150
2	資安設備_網路防火牆	低階	300
		高階	500
3	郵件管理過濾機制		150
4	資安設備_IDS	低階	150
		高階	450
5	資安設備_IPS	低階	250
		中階	300
		高階	500
6	資安設備_應用程式防火牆(WAF)	低階	300
		中階	400

序號	日誌種類	型式	EPS
		高階	1500
7	資安設備_APT 防禦措施		150
8	網站主機	低階	300
		高階	500
9	網路設備(路由器)		250
10	代理伺服器		250
11	郵件伺服器		200
12	目錄伺服器		150
13	檔案伺服器		150
14	資料庫伺服器		500
15	DNS 伺服器	低階	150
		高階	250

（二）計價方式

項目	單位	服務所需人天	SOC 監控服務-中流量服務總金額
1. SOC 監控環境部署 2. 監控服務 3. 資安事件處理 4. 資安威脅預警	**1 年服務**	365	(365*人天費率)

註：1 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。

（三）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器安裝、網段部

署、設定、系統調校與重要資安事件 Rule 導入等工作。

（2）Event 數量計算以事件收集器所收集的數量為基準；廠商應每季檢視受監控設備之 EPS 情形，檢視監控部署執行成效，適時提出部署調整建議。

（3）廠商發現事件收集器故障，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。

（4）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，每次應於 24 小時內完成修復。

（5）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，機關應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。

（6）若機關有調整監控設備部署之需求，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）廠商收集日誌後，透過資安監控機制進行整合與關聯，產生「資安監控單」(例如：Incident)。

（2）SOC 分析人員對「資安監控單」進行影響性評估，並產生「情資分析單」(例如:Ticket)，廠商應即時以適當方式(以電話、手機簡訊、電子郵件、網頁、傳真等)通知機關資安連絡人，俾利機關進行情資處理。

（3）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」辦理下列事項：

A、連通測試：

廠商應通過資安聯防監控情資連通測試，尚未通過連通測試者，應填寫「資安情資回傳連通測試申請單」，提出申請並通過連通測試，確保廠商之情資回傳能力。

B、正式回傳作業辦理：

廠商應協助機關即時回傳資安監控服務之「資安監控單」

與「情資分析單」至指定之聯防監控平台；另依據監控設備之監控狀況，每月提交「監控設備狀況單」至指定之聯防監控平台。

C、聯防監控情資有效性檢核

廠商應確保資安監控偵測與分析、資安情資回傳、資安監控情資內容品質之有效性。

D、廠商應確實協助公務機關配合政府領域聯防監控作業，除上述辦理事項外，亦應遵照機關其所屬領域主管機關訂定之作業規範，配合辦理 SOC 監控資訊回傳作業。

E、「資安監控單」、「情資分析單」及「監控設備狀況單」等表單格式應依行政院國家資通安全會報技術服務中心網站 https://www.nccst.nat.gov.tw/GSOC 公告之聯防監控資安情資回傳 STIX 格式規範。

（4）廠商應定期提交月報、季報、年報予機關，月報得以紙本文件或電子檔、網頁型式等方式提交，而季報、年報則應到府進行提報。

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包括：

A、廠商必須進行受駭根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資料蒐集，日誌檢視以 1 年為原則(含線上與離線日誌)。

C、針對蒐集的資料進行資料保存、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：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、Security Focus、各國 CERT(如 CISA(USCERT))及 MITRE 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，整理相關訊息通知機關，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。

（四）相關服務人員資格

1. 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 1)。

2. 資安事件處理人員，應具備必要之各類資訊網路、系統技能，接受過 CEH(Certified Ethical Hacker)或 ECIH(EC-Council Incident Handler)資安危機處理員認證或其他類似相關課程訓練證明(以上訓練證明擇 1)。

3. 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採購機關同意後始得服務。

4. 服務人員須年滿 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。

（五）廠商應交付文件及辦理項目：

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. 配合機關辦理至少 1 次說明會議。

（六）交付文件基本要求

1. SOC 監控設備部署建議報告

（1）提出工作計畫書，包括各項工作執行規劃、監控設備部署規劃、監控與警示作業之方式、通知機關資安連絡人之時機、內容及方式、資安事件處理之作業、資安威脅預警之作業等。

（2）各項報告(月報、季報、年報)提交時間及內容。

2. SOC 監控服務月報

（1）監控與警示情形，除依規定時間通知機關與回傳指定之聯防監控平台外，亦應於機關之相關報告呈現。

A、當月「資安監控單」之產生數量及回傳數量等資訊。

B、當月「情資分析單」之產生數量、回傳數量及通知機關數量等資訊；另詳列「情資分析單」內容，包括表單編號、事件主旨、事件類別、觸發規則、來源 IP、目的 IP、事件描述、影響等級等與情資分析單有關之資訊。

C、當月之「監控設備狀況單」，呈現其監控設備運作情形。

D、監控情資之統計分析：（以下為基本要求，廠商或機關可再酌增項目）

a. 當月「情資分析單」之事件主旨、事件類別、觸發規則之統計分析。

b. 外部威脅連線 IP 清單，清整當月外部威脅連線 IP，可用於黑名單阻擋以利後續追蹤。

c. 其他。

A、 機關之資安弱點及強化措施建議。

（2）資安事件處理

當月協助處理資安事件之彙整資訊及處理進度說明，詳細資安事件處理之報告以分件撰寫報告。

（3）資安威脅預警

A、 當月資安威脅預警分類彙整，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。

B、 建議設置防禦之措施及提供資安威脅預警諮詢服務紀錄。

（4）總結

3. SOC 監控服務季報

彙整當季之 SOC 監控、資安事件處理、資安威脅預警之重點，並

且提出相關之統計、趨勢分析及強化防護建議，包括：

（1）監控與警示分析

A、 當季統計分析：(以下為基本要求，廠商或機關可再酌增項目)

a. 當季「資安監控單」、「情資分析單」之統計，包括事件主旨、事件觸發規則及事件類別統計，說明近期機關遭受資安威脅趨勢。

b. 外部威脅連線 IP 清單，清整當季外部威脅連線 IP，可用於黑名單阻擋以利後續追蹤。

c. 其他

B、 提供當季受監控設備之 EPS 資訊，檢視監控部署執行成效，適時提出部署調整建議。

C、 綜整機關威脅趨勢、資安弱點及強化措施建議。

（2）資安事件處理

當季協助處理資安事件之彙整資訊及處理進度說明，詳細資安事件處理之報告以分件撰寫報告。

（3）資安威脅預警

A、 資安威脅預警之分類與數量。

B、 資安威脅重大預警重點摘要。

C、 資安威脅預警趨勢分析。

D、 機關可預防之建議。

（4）總結

4. SOC 監控服務年報

（1）監控與警示分析

A、 年統計分析：(以下為基本要求，廠商或機關可再酌增項目)

a. 事件主旨、觸發規則、事件類別統計等，說明近 1 年機關遭受資安威脅趨勢。

b. 外部威脅連線 IP 清單，清整近 1 年外部威脅連線 IP，可用

於黑名單阻擋以利後續追蹤。

c. 其他

B、 綜整近 1 年機關之威脅趨勢、資安弱點及強化措施建議。

C、 全年受監控資安設備之 EPS 統計，以供機關了解資安設備之處理效能，作為後續採購或監控部署之參考。

（2）資安事件處理

年度協助處理資安事件之彙整資訊及處理進度說明，詳細資安事件處理之報告以分件撰寫報告。

（3）資安威脅預警分析

A、 資安威脅預警整合分析。

B、 資安威脅重大預警重點摘要。

C、 資安威脅預警整合分析，並提出趨勢預測。

D、 機關可預防之建議。

（4）總結

5. 資安事件處理報告(分件撰寫報告)

針對各別資安事件之基本資訊，與資安事件處理等過程進行紀錄，並提出矯正預防措施建議，包括精進內部程序文件、強化安全防護、提升教育訓練等建議，以提升機關之防護能量。

（1）資安事件之基本資訊說明，包括事件編號、事件主旨、事件分級、發現時間、通報時間、受駭標的資料、事件類別、事件說明等。

（2）資安事件處理之根因調查及後續改善建議，包括資料蒐集、資料分析、根因分析、駭客入侵手法、入侵時間、影響範圍及後續追蹤改善項目等。

（七）機關配合事項

機關應提供適當環境配合 SOC 監控環境部署。

二、第 2 組資通安全威脅偵測管理(SOC)服務

第 3 項：資通安全威脅偵測管理(SOC)服務-高流量

資通安全威脅偵測管理(SOC)服務提供網通設備、資安防護措施(如防毒軟體、網路防火牆、應用程式防火牆、APT 防禦措施、電子郵件過濾及 IDS/IPS 等)、主機伺服器等資安事件監控、事件處理、資安威脅預警等服務。透過監控及分析，可將監控設備所產生的日誌，以系統化方式進行收集、關聯性分析後，提供給機關進行情資管理。

（一）監控服務處理效能：

1. 受監控設備之整體處理效能總達 4900 EPS(Event Per Second)。
2. 監控 EPS 以日誌種類、設備數量推算所得，機關訂購前先參考機關過去 3 年之資安設備實際的 EPS 或表 3 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。
3. SOC 監控設備應納入資通安全責任等級分級辦法之資通安全防護措施(包括防毒軟體、網路防火牆、電子郵件過濾機制、IDS/IPS、應用程式防火牆及 APT 防禦措施等)，及機關之核心資通系統(含 AD)等資訊設備紀錄與服務/應用程式紀錄（應以上列整體處理效能 EPS 為原則）。

表 3 日誌種類參考表

序號	日誌種類	型式	EPS
1	防毒軟體(防毒伺服器，防毒閘道器)		150
2	資安設備_網路防火牆	低階	300
		高階	500
3	郵件管理過濾機制		150
4	資安設備_IDS	低階	150
		高階	450
5	資安設備_IPS	低階	250
		中階	300
		高階	500
6	資安設備_應用程式防火牆(WAF)	低階	300
		中階	400

序號	日誌種類	型式	EPS
		高階	1500
7	資安設備_APT 防禦措施		150
8	網站主機	低階	300
		高階	500
9	網路設備(路由器)		250
10	代理伺服器		250
11	郵件伺服器		200
12	目錄伺服器		150
13	檔案伺服器		150
14	資料庫伺服器		500
15	DNS 伺服器	低階	150
		高階	250

（二）計價方式

項目	單位	服務所需人天	SOC 監控服務- 高流量服務總金額
1. SOC 監控環境部署 2. 監控服務 3. 資安事件處理 4. 資安威脅預警	**1 年服務**	365	(365*人天費率)

註:1 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。

（三）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器安裝、網段部署、設定、系統調校與重要資安事件 Rule 導入等工作。

（2）Event 數量計算以事件收集器所收集的數量為基準；廠商應每

季檢視受監控設備之 EPS 情形，檢視監控部署執行成效，適時提出部署調整建議。

（3）廠商發現事件收集器故障，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。

（4）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，每次應於 24 小時內完成修復。

（5）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。

（6）若機關有調整監控設備部署之需求，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）廠商收集日誌後，透過資安監控機制進行整合與關聯，產生「資安監控單」(例如：Incident)。

（2）SOC 分析人員對「資安監控單」進行影響性評估，並產生「情資分析單」(例如:Ticket)，廠商應即時以適當方式(以電話、手機簡訊、電子郵件、網頁、傳真等)通知機關資安連絡人，俾利機關進行情資處理。

（3）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」辦理下列事項：

A、連通測試：

廠商應通過資安聯防監控情資連通測試，尚未通過連通測試者，應填寫「資安情資回傳連通測試申請單」，提出申請並通過連通測試，確保廠商之情資回傳能力。

B、正式回傳作業辦理：

廠商應協助機關即時回傳資安監控服務之「資安監控單」與「情資分析單」至指定之聯防監控平台；另依據監控設備之監控狀況，每月提交「監控設備狀況單」至指定之聯

防監控平台。

C、聯防監控情資有效性檢核：

廠商應確保資安監控偵測與分析、資安情資回傳、資安監控情資內容品質之有效性。

D、廠商應確實協助公務機關配合政府領域聯防監控作業，除上述辦理事項外，亦應遵照機關其所屬領域主管機關訂定之作業規範，配合辦理 SOC 監控資訊回傳作業。

E、「資安監控單」、「情資分析單」及「監控設備狀況單」等表單格式應依行政院國家資通安全會報技術服務中心網站 https://www.nccst.nat.gov.tw/GSOC 公告之聯防監控資安情資回傳 STIX 格式規範。

（4）廠商應定期提交月報、季報、年報予機關，月報得以紙本文件或電子檔、網頁型式等方式提交，而季報、年報則應到府進行提報。

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、廠商必須進行受駭根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資料蒐集，日誌檢視以 1 年為原則(含線上與離線日誌)。

C、針對蒐集的資料進行資料保存、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：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、Security Focus、各國 CERT(如 CISA(USCERT))及 MITRE 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，整理相關訊息通知機關，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。

（四）相關服務人員資格

1. 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 1)。

2. 資安事件處理人員，應具備必要之各類資訊網路、系統技能，接受過 CEH(Certified Ethical Hacker)或 ECIH(EC-Council Incident Handler)資安危機處理員認證或其他類似相關課程訓練證明(以上訓練證明擇 1)。

3. 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採購機關同意後始得服務。

4. 服務人員須年滿 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。

（五）廠商應交付文件及辦理項目：

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. 配合機關辦理至少 1 次說明會議。

（六）交付文件基本要求

1. SOC 監控設備部署建議報告

（1）提出工作計畫書，包括各項工作執行規劃、監控設備部署規劃、監控與警示作業之方式、通知機關資安連絡人之時機、內容及方式、資安事件處理之作業、資安威脅預警之作業等。

（2）各項報告(月報、季報、年報)提交時間及內容。

2. SOC 監控服務月報

（1）監控與警示情形，除依規定時間通知機關與回傳指定之聯防監控平台外，亦應於機關之相關報告呈現。

A、當月「資安監控單」之產生數量及回傳數量等資訊。

B、當月「情資分析單」之產生數量、回傳數量及通知機關數量等資訊；另詳列「情資分析單」內容，包括表單編號、事件主旨、事件類別、觸發規則、來源 IP、目的 IP、事件描述、影響等級等與情資分析單有關之資訊。

C、當月之「監控設備狀況單」，呈現其監控設備運作情形。

D、監控情資之統計分析：（以下為基本要求，廠商或機關可再酌增項目）

a. 當月「情資分析單」之事件主旨、事件類別、觸發規則之統計分析。

b. 外部威脅連線 IP 清單，清整當月外部威脅連線 IP，可用於黑名單阻擋以利後續追蹤。

c. 其他。

A、 機關之資安弱點及強化措施建議。

（2）資安事件處理

當月協助處理資安事件之彙整資訊及處理進度說明，詳細資安事件處理之報告以分件撰寫報告。

（3） 資安威脅預警

A、 當月資安威脅預警分類彙整，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。

B、 建議設置防禦之措施及提供資安威脅預警諮詢服務紀錄。

（4）總結

3. SOC 監控服務季報

彙整當季之 SOC 監控、資安事件處理、資安威脅預警之重點，並且提出相關之統計、趨勢分析及強化防護建議，包括：

（1）監控與警示分析

A、 當季統計分析（以下為基本要求，廠商或機關可再酌增項目）：

a. 當季「資安監控單」、「情資分析單」之統計，包括事件主旨、事件觸發規則及事件類別統計，說明近期機關遭受資安威脅趨勢。

b. 外部威脅連線 IP 清單，清整當季外部威脅連線 IP，可用於黑名單阻擋以利後續追蹤。

c. 其他

B、 提供當季受監控設備之 EPS 資訊，檢視監控部署執行成效，適時提出部署調整建議。

C、 綜整機關威脅趨勢、資安弱點及強化措施建議。

（2）資安事件處理

當季協助處理資安事件之彙整資訊及處理進度說明，詳細資安事件處理之報告以分件撰寫報告。

（3）資安威脅預警

A、 資安威脅預警之分類與數量。

B、 資安威脅重大預警重點摘要。

C、 資安威脅預警趨勢分析。

D、 機關可預防之建議。

（4）總結

4. SOC 監控服務年報

（1）監控與警示分析

A、 年統計分析：（以下為基本要求，廠商或機關可再酌增項目）

a. 事件主旨、觸發規則、事件類別統計等，說明近 1 年機關遭受資安威脅趨勢。

b. 外部威脅連線 IP 清單，清整近 1 年外部威脅連線 IP，可用於黑名單阻擋以利後續追蹤。

c. 其他

B、 綜整近 1 年機關之威脅趨勢、資安弱點及強化措施建議。

C、 全年受監控資安設備之 EPS 統計，以供機關了解資安設備之處理效能，作為後續採購或監控部署之參考。

（2）資安事件處理

全年協助處理資安事件之彙整資訊及處理進度說明，詳細資安事件處理之報告以分件撰寫報告。

（3）資安威脅預警分析

A、 資安威脅預警整合分析。

B、 資安威脅重大預警重點摘要。

C、 資安威脅預警整合分析，並提出趨勢預測。

D、 機關可預防之建議。

（4）總結

5. 資安事件處理報告(分件撰寫報告)

針對各別資安事件之基本資訊，與資安事件處理等過程進行紀錄，並提出矯正預防措施建議，包括精進內部程序文件、強化安全防護、提升教育訓練等建議，以提升機關之防護能量。

（1）資安事件之基本資訊說明，包括事件編號、事件主旨、事件分級、發現時間、通報時間、受駭標的資料、事件類別、事件說明等。

（2）資安事件處理之根因調查及後續改善建議，包括資料蒐集、資料分析、根因分析、駭客入侵手法、入侵時間、影響範圍及後續追蹤改善項目等。

（七）機關配合事項

機關應提供適當環境配合 SOC 監控環境部署。

三、第 3 組弱點檢測服務

針對主機系統、Web 網頁安全弱點、網頁個資檢測，可評估檢測標的物是否存在安全弱點或個資特徵，提供給機關相關檢測結果，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. 檢測服務細項：分為主機系統弱點檢測、Web 網頁弱點檢測及網頁個資檢測。

（1）主機系統弱點檢測

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，系統弱點檢測的檢測項目，應符合 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 網頁弱點檢測

針對機關對外主機網頁安全弱點進行檢測，檢測項目應符合 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

（3）網頁個資檢測

針對機關對外網頁與網頁中之 doc(x)、xls(x)、ppt(x)、pdf、csv 等類型檔案，可能存在之個人資料進行檢測，檢測個資特徵應至少包含中文姓名、地址、電話(含市話和手機)、電子郵件信箱、中華民國身分證字號、護照和信用卡號等個人資料檢測。廠商僅將存在個資特徵之網頁資訊及哪些個資特徵及數量，彙整成報告，並提醒機關應檢視被檢測出之個資特徵揭露之合宜性。

2. 檢測次數

於訂購後半年內，依機關採購項目提供以下服務次數：

服務細項	次數
主機系統弱點檢測	2 次檢測(初測、複測)
Web 網頁弱點檢測	2 次檢測(初測、複測)
網頁個資檢測	1 次檢測

3. 檢測方式

檢測工具應取得合法授權使用的軟體或工具，於非公務時段或與機關協調取得適當時間進行檢測作業。

4. 分析報告

檢測作業後 1 個月內，根據檢測結果，將所發現之弱點與過程詳細記錄，並對結果進行分析，提出相關建議與檢測報告，以提供作為弱點修補之參考。

（二）計價方式

項次	項目	單位	服務所需人天	最低採購量	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)
1	主機系統弱點檢測-到場服務	IP	0.35	15	0	0	
2	主機系統弱點檢測-遠端服務	IP	0.3	10	100	30	
3	WEB 網頁弱點檢測(WebVA)-到場服務	URL	3	1	0	0	
4	WEB 網頁弱點檢測(WebVA)-遠端服務	URL	2	1	10	20	
5	網頁個資檢測-遠端服務	URL	1	1	1	1	
	採購總人天						

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)

（三）計價方式說明：

1. 弱點檢測服務，機關可依需求分項選購，且應依分項之最低採購數量原則進行採購。
2. 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）弱點檢測服務人員資格

參與弱點檢測服務人員應具備以下所列舉之技能，以確保服務水準。

1. 弱點檢測服務人員，應具備必要之各類資訊網路、系統技能，熟悉弱點檢測工具與檢測結果判讀能力，接受過 CEH(Certified Ethical Hacker)或其他類似相關課程訓練證明(以上訓練證明擇 1)。
2. 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。
3. 服務人員須年滿 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。

（五）廠商應交付文件及辦理項目

1. 弱點檢測服務報告(初測與複測均應提供)。
2. 配合機關初測與複測原則上各辦理 1 次說明會議(視機關需求)。

（六）交付文件基本要求

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）整體結果統計說明。
   （2）檢測時間、檢測方式、檢測工具說明。
   （3）弱點發現及改善建議：針對各項檢測結果，詳列驗證後確實存在之弱點名稱、風險等級、弱點說明、修補建議、參考來源及受影響之檢測使用者電腦 IP，以利機關瞭解弱點可能造成之影響並進行修補與追蹤。
   （4）網頁個資檢測情形：針對網站之內容進行個人資料之特徵資訊檢測，將存在個資特徵之網頁資訊及哪些個資特徵及數量，彙整成報告，並提醒機關檢視個資揭露之合宜性。
4. 結論

（七）機關配合事項

檢測與複掃作業時間機關與廠商協調取得適當時間進行。

四、第 4 組滲透測試服務

滲透測試係透過模擬有心人士之攻擊方式，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、連接網際網路(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。

滲透測試執行方式分為內網滲透測試及外網滲透測試。

1. 資料蒐集

對受測目標進行資料蒐集與資訊分析，將取得之相關資訊做為執行滲透測試決策。

2. 測試次數

訂購後半年內，提供機關 2 次滲透測試服務(初測與複測)。

3. 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(過程與結果應有佐證畫面)，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，對於不適用之測試項目，應註明並說明不適用理由。

4. 風險管理

在滲透測試執行期前，應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應與機關進行確認，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。

5. 系統滲透測試項目

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

測試類型	測試類別	測試項目
	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
	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

測試類型	測試類別	測試項目
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

6. 物聯網設備滲透測試項目

物聯網設備滲透測試以外網滲透測試為主，依檢測之物聯網設備類別，測試其開啟之服務是否存在弱點，若有不適用之測試類別，應註明並說明不適用理由。

測試類型	測試類別	測試項目
系統	本機服務	針對物聯網設備與管理主機，執行服務套件弱點測試等項目
網站服務	設定管理	包含應用程式設定測試、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	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	包含 Session 管理測試、Cookie 屬性測試、Session 資料更新測試及 Session 變數傳遞測試等項目
	使用者授權	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	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	包含 XSS 漏洞測試、SQL Injection 測試及 Code Injection 測試等項目
應用	網站服務	包含常見 WEB 套件弱點測試，如設定缺失、權限

程式	套件	控管及套件弱點等測試項目
	遠端連線服務套件	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
	其它	包含 SMB、LPD、IPP、Jetdirect、SNMP 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	包含 WEB、FTP、SSH、TELNET、RDP、VNC 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	針對無線網路基地台/無線路由器設備，執行包含無線服務套件弱點測試、無線通訊協定及 WiFi 密碼字典檔測試等項目

7. 物聯網設備配套檢測參考:

項次	物聯網設備類型	設備檢測範圍
1	網路印表機	網路印表機
2	網路攝影機	網路攝影機、網路影像錄影機(NVR)、影像管理主機等
3	門禁設備	指紋機、門禁卡機、門禁管理主機等
4	無線網路基地台/無線路由器	無線網路基地台、無線路由器、無線區域網路控制器、Thin AP 等
5	環控系統	智慧溫度計、智慧溼度計、環控伺服器等
6	其他物聯網設備	視物聯網類型而定

（二）計價方式

項次	項目	單位	服務所需人天	最低採購量	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)
1	內網滲透測試-	URL	16	1	1	16	

項次	項目	單位	服務所需人天	最低採購量	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)
	到場服務	或 IP					
2	外網滲透測試-遠端服務	URL 或 IP	15	1	0	0	
3	物聯網設備內網滲透測試_到場服務	IP	1.6	10	10	16	
4	物聯網設備外網滲透測試_遠端服務	IP	1.5	10	0	0	
	採購總人天						

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)

（三）計價方式說明：

1. 滲透測試服務，機關可依需求分項選購，且應依分項之最低採購數量原則進行採購。
2. 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）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。

1. 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 Certified Security Analyst (ECSA)或其他類似相關課程訓練(以上訓練證明擇 1)。

（2）滲透測試服務：接受過 GPEN (GIAC Certified Penetration Tester)、GWAPT(GIAC Web Application Penetration Tester)、OSCP(Offensive Security Certified Professional)、LPT(Licensed Penetration Tester)或其他類似相關課程訓練證明(以上訓練證明擇 1)。

2. 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。

3. 服務人員須年滿 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。

（五）廠商應交付文件及辦理項目

1. 滲透測試服務報告。(初測與複測均應提供)

2. 配合機關初測與複測原則上各辦理 1 次說明會議(視機關需求)。

（六）交付文件基本要求

1. 執行計畫

執行期間/執行項目/執行範圍/專案成員。

2. 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)

3. 滲透測試弱點發現與改善建議(各個檢測項目分開撰寫)

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)，應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。

（1）說明資通系統/物聯網設備之檢測資訊，如：Web AP、DB 與 Server 之網域名稱、IP 及設備開啟之服務埠等。

（2）檢測結果，分別詳列弱點主機之 IP 或網域名稱、弱點名稱、風險等級、CVE 編號、弱點分類、弱點說明、修補建議、檢測說明及檢測畫面等。

A、 資訊內容應包含檢測人員如何發現弱點所在頁面與採用之攻擊手法，針對測試結果可能導致的風險或可能洩漏的資訊內容，以及攻擊成功之檢測畫面與攻擊過程描述。

B、 著重於弱點修補建議，以利機關快速掌握弱點成因與影響範圍，並參考改善方式進行修復。

4. 結論

（七）機關配合事項

執行作業時間機關與廠商協調取得適當時間進行，測試標的(IP/Domain)應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 組社交工程演練服務

社交工程演練包括電子郵件測試及簡訊測試服務，係透過電子郵件/簡訊的方式提供受測機關瞭解社交工程的存在，並提高警覺性；同時受測機關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(分項採購)

服務項目/服務內容	1.電子郵件測試服務	2.簡訊測試服務
測試次數與規格	1. 訂購後 1 年內，提供機關電子郵件帳號 2 次的測試。 2. 各帳號進行 5 封社交工程郵件測試，包括本文、附件、可連結資訊。	1. 訂購後 1 年內，提供機關手機門號 2 次的測試。 2. 各門號進行 5 封社交工程簡訊測試。
測試內容	1. 社交工程郵件設計應涵蓋 3 種以上不同類型的內容，例如：八卦、休閒、保健、財經、情色、新奇、時事等資訊。 2. 記錄「開啟郵件」、「點閱連結」及「開啟附件」等受測者行為。	1. 社交工程簡訊設計應涵蓋 3 種以上不同類型的內容，例如：八卦、休閒、保健、財經、情色、新奇、時事等資訊。 2. 記錄「點閱簡訊內容之連結」受測者行為。
分析報告	1. 整體結果統計圖表，不同類型內容/分組結果/排序統計表。(說明測試內容、分類及各類的檢測結果及排序統計) 2. 郵件派送時間表。 3. 統計「開啟郵件」、「點閱連結」及「開啟附件」等受測	1. 整體結果統計圖表，不同類型內容/分組結果/排序統計表。(說明測試內容、分類及各類的檢測結果及排序統計) 2. 簡訊派送時間表。 3. 統計「點閱簡訊內容之連結」之受測者行為。 4. 統計「點閱簡訊內容之連結

服務項目/服務內容	1.電子郵件測試服務	2.簡訊測試服務
	者行為。 4. 統計「郵件開啟率」、「郵件點閱率」及「開啟附件率」等結果。 5. 受測者開啟與點閱細部時間紀錄。	率」等結果。 5. 受測者點閱細部時間紀錄。
諮詢服務	分析報告提出後 1 個月內提供 8x5 諮詢服務。	分析報告提出後 1 個月內提供 8x5 諮詢服務。

（二）計價方式

項次	服務項目	單位	服務所需人天	單項服務金額(服務所需人天*人天費率)
1	電子郵件測試服務	100 個電子郵件帳號 (1~100)	10	
		200 個電子郵件帳號 (101~200)	11	
		500 個電子郵件帳號 (201~500)	13	
		1000 個電子郵件帳號 (501~1000)	15	
2	簡訊測試服務	50 個手機門號 (1~50)	9 (含簡訊費用)	
		100 個手機門號 (51~100)	10 (含簡訊費用)	
		200 個手機門號 (101~200)	11 (含簡訊費用)	
		500 個手機門號	13	

項次	服務項目	單位	服務所需人天	單項服務金額(服務所需人天*人天費率)
		(201~500)	(含簡訊費用)	
		1000 個手機門號 (501~1000)	15 (含簡訊費用)	
	採購總人天			

註: 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)

（三）計價方式說明：

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/簡訊數量超過 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。
2. 社交工程演練服務，機關可依需求分項選購，且應依分項之最低採購數量原則進行採購。
3. 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）社交工程演練服務人員資格

參與社交工程演練服務人員，應具備以下所列舉之技能，以確保服務水準。

1. 社交工程演練服務人員，應具備必要之各類資訊網路、系統技能，接受過 CEH(Certified Ethical Hacker)或其他類似相關課程訓練證明(以上訓練證明擇 1)。
2. 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。
3. 服務人員須年滿 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。

（五）廠商應交付項目及配合事項

1. 社交工程演練服務_電子郵件/簡訊測試報告。
2. 配合機關辦理至少 1 次說明會議。

（六）廠商執行服務前注意事項

為避免資通安全社交工程郵件測試服務所寄送之演練郵件，經惡意電郵威脅分析機制觸發造成誤判，影響機關演練結果與廠商服務品質，請資安服務廠商每次執行前均需先通知技服中心，提供社交工程郵件檢測服務之相關資訊，以明確紀錄機關社交工程演練之執行成效。相關作業說明如下：

1. 提供社交工程檢測電子郵件測試之寄送資訊，包括：執行時間、寄送來源 IP 位址、回報連線 IP 位址與 FQDN 網域名稱、寄件者帳號、採購機關名稱。
2. 提供方式：將上述資訊以 xls、xlsx 資料表檔案，透過郵件寄送至 mute@nccst.nat.gov.tw;

(1)郵件主旨如下：

主旨：〔廠商名稱〕共契服務_109 年社交工程演練_電子郵件測試資訊。

(2)資料表範例如下：

執行時間	寄送來源 IP 位址	回報連線 IP 位址 /FQDN 網域名稱	寄件者帳號	採購機關名稱
起：109/11/1 迄：109/12/01	123.123.123.123	111.111.111.111 se-mail_link.com	test@mail.com .tw	某機關

3. 提供時間：服務執行至少 2 週前提供，以利調整作業。

（七）文件報告基本要求(依採購項目撰寫)

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

電子郵件測試	簡訊測試
1. 整體結果統計圖表，不同類型內容/分組結果/排序統計表。 2. 郵件派送時間表。 3. 統計「開啟郵件」、「點閱連結」及「開啟附件」等受測者行為。 4. 統計「郵件開啟率」與「郵件點閱率」及「開啟附件率」等結果。 5. 受測者開啟與點閱細部時間紀錄。	1. 整體結果統計圖表，不同類型內容/分組結果/排序統計表。 2. 簡訊派送時間表。 3. 統計「點閱簡訊內容之連結」之受測者行為。 4. 統計「點閱簡訊內容之連結率」之結果 5. 受測者點閱細部時間紀錄。

4. 結果建議

針對各項結果，提出改善建議。

5. 結論

（八）機關配合事項

執行作業時間機關與廠商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紀錄報表，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，並彙整紀錄於每月服務報告。

(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，並彙整紀錄於每月服務報告。

(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，並彙整紀錄於每月服務報告。

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，並彙整紀錄於每月服務報告。

6. 服務監控

提供每月網路防火牆服務監控報告，提供報告內容須包含以下項目：

(1) 網路流量統計紀錄

(2) 網路資安威脅統計紀錄

(3) 網路資安告警紀錄

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、NCC 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 100 Mbps。
   (2) UTM 整合式威脅管理處理流量可達 300 Mbps。
   (3) UTM 整合式威脅管理處理流量可達 500 Mbps。
   (4) UTM 整合式威脅管理處理流量可達 1Gbps。
3. VPN 效能具備可同時建立 8 條(含)以上 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或支援即時資安分析與通報服務，協助分析潛在的惡意連線與病毒，並提供即時的通報服務，提升單位內的防禦與偵測能力，降低資安攻擊事件發生的機率。
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。

(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。