

113 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檢視服務，除包含網路架構檢視、網路惡意活動檢視、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視、目錄伺服器設定及防火牆連線設定檢視等資安法規定之資安健診項目外，另包含政府組態基準(GCB)檢視、資料庫安全檢視等其他項目，提供機關資安改善建議，藉以落實技術面與管理面相關控制措施，以提升網路與資通系統安全防護能力。

(一) 服務項目

服務項目		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 網路設備紀錄檔分析	1.檢視網路設備紀錄檔(如防火牆、入侵偵測/防護系統等)，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.網路設備紀錄檔分析以 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 使用者端電腦更新檢視	1.檢視使用者端電腦之 Microsoft 作業系統更新情形 2.檢視使用者端電腦之應用程式之安全性更新情形(包含 Office 應用程式舉凡 word、powerpoint、Excel、Access 等、Adobe Acrobat 及 Java 應用程式等)

服務項目		內容說明
		<p>3.檢視使用者端電腦是否使用已經終止支援之作業系統或軟體(如 Windows XP、Windows7、Office 2003、Office 2007、Adobe Flash Player 等，依使用作業系統或軟體之官網公告資訊為主)，針對使用終止支援之軟體，建議其停用並移除</p> <p>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</p>
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	<p>1. 檢視伺服器之 Microsoft 作業系統更新情形</p> <p>2. 伺服器之應用程式之安全性更新情形(包含 Office 應用程式舉凡 word、powerpoint、Excel、Access... 等、Adobe Acrobat 及 Java 應用程式)</p> <p>3. 檢視伺服器是否使用已經終止支援之作業系統或軟體(如 Windows Server 2003、Office 2003、Office 2007、Adobe Flash Player 等，依使用作業系統或軟體之官網公告資訊為主)，針對使用終止支援之軟體，建議其停用並移除</p> <p>4. 檢視伺服器是否使用不合宜之作業系統(如使用 Windows 7、Windows10 等)</p> <p>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</p>
5.目錄伺服器設定檢視		<p>1. 針對 AD 伺服器組態設定，依國家資通安全研究院官方網站「政府組態基準(GCB)」專區之 GCB 說明文件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</p> <p>2. 參考網址為 https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/GCB/ </p> <p>3. 作為 AD server 之伺服器其 GCB 設定皆應檢視</p>
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)

服務項目	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	<ul style="list-style-type: none"> • 針對使用者電腦組態設定檢視，依國家資通安全研究院官方網站「政府組態基準(GCB)」專區之 GCB 說明文件之作業系統說明文件所公布的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.nics.nat.gov.tw/core_business/cybersecurity_defense/GCB/
	7.2 作業系統_伺服器組態設定檢視	<ul style="list-style-type: none"> • 針對伺服器組態設定檢視，依國家資通安全研究院官方網站「政府組態基準(GCB)」專區之 GCB 說明文件之作業系統說明文件所公布的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.nics.nat.gov.tw/core_business/cybersecurity_defense/GCB/
	7.3 瀏覽器組態設定檢視	<ul style="list-style-type: none"> • 針對瀏覽器之組態設定檢視，依國家資通安全研究院官方網站「政府組態基準(GCB)」專區之 GCB 說明文件之瀏覽器說明文件所公布的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.nics.nat.gov.tw/core_business/cybersecurity_defense/GCB/
	7.4 網通設備組態設定檢視	<ul style="list-style-type: none"> • 針對網通設備組態設定檢視，依國家資通安全研究院官方網站「政府組態基準(GCB)」專區之 GCB 說明文件之網通設備說明文件所公布的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.nics.nat.gov.tw/core_business/cybersecurity_defense/GCB/

服務項目	內容說明	
		siness/cybersecurity_defense/GCB/
	7.5 應用程式組態設定檢視	<ul style="list-style-type: none"> 針對應用程式組態設定檢視，依國家資通安全研究院官方網站「政府組態基準(GCB)」專區之 GCB 說明文件之應用程式說明文件所公布的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.nics.nat.gov.tw/core_business/cybersecurity_defense/GCB/
8.資料庫安全檢視	8.1 特權帳號管理	<ul style="list-style-type: none"> 資料庫安全檢視標的，以機關具所有權或管理權之資料庫為主 以強化資料庫安全防護角度，依據機關內部之資安管理機制(包含文件程序及紀錄等)，檢視其適法性、防護強度及落實情形，並提供專業建議 包含 7 大檢視類別、30 項檢視項目，以訪談與實機檢視方式，確認資料庫防護狀況，詳見資料庫安全檢視
	8.2 資料加密	
	8.3 存取授權	
	8.4 稽核紀錄	
	8.5 委外管理	
	8.6 備份保護	
	8.7 弱點管理	

表1 資料庫安全檢視項目要求

類別	項次	檢視項目	檢視要求
8.1 特權帳號管理	1	變更資料庫預設管理帳號	<ul style="list-style-type: none"> 訪談資料庫帳號權限管理機制 實機檢視資料庫帳號權限列表，確認預設管理帳號已變更
	2	啟用帳號鎖定次數	<ul style="list-style-type: none"> 訪談資料庫角色與權限劃分機制、帳號管理及密碼設定規範 實機檢視資料庫特權帳號鎖定次數，確認符合機關規定

類別	項次	檢視項目	檢視要求
	3	啟用帳號鎖定時間	<ul style="list-style-type: none"> 訪談資料庫角色與權限劃分機制、帳號管理及密碼設定規範 實機檢視資料庫特權帳號鎖定時間，確認符合機關規定
	4	啟用密碼複雜度原則	<ul style="list-style-type: none"> 訪談資料庫角色與權限劃分機制、帳號管理及密碼設定規範 實機檢視資料庫特權帳號密碼複雜度(英數字、大小寫、特殊符號)設定規則，確認符合機關規定
	5	啟用密碼長度原則	<ul style="list-style-type: none"> 實機檢視資料庫特權帳號密碼設定長度，確認符合機關規定
	6	啟用密碼最長有效期限原則	<ul style="list-style-type: none"> 實機檢視資料庫特權帳號密碼有效期限設定天數，確認符合機關規定
	7	限制管理者帳號透過遠端存取	<ul style="list-style-type: none"> 訪談資料庫管理者遠端連線機制 檢視資料庫遠端連線設定、連線授權紀錄，避免資料庫管理者從非管理網段進行管理作業
8.2 資料加密	8	資料庫資料具有適當保護機制(包含加密、不可識別處理)	<ul style="list-style-type: none"> 訪談資料庫資料保護機制(如加密方式、保護資料範圍、不可識別處理之方式等) 實機檢視資料庫資料之加密設定、加密結果、不可識別處理之結果
	9	資料庫資料具有安全傳輸機制	<ul style="list-style-type: none"> 訪談資料庫傳輸保護機制 實機檢視資料庫資料傳輸加密方式與設定狀況，避免採用不安全的資料傳輸方式
	10	資料庫加密金鑰具有適當保護機制	<ul style="list-style-type: none"> 訪談資料庫加密金鑰管理機制(如使用狀況、保管情形等) 檢視資料庫金鑰存取相關申請、審核紀錄及金鑰管理方式，避免遭非授權人員存取
8.3 存取授權	11	限制資料庫主機服務埠	<ul style="list-style-type: none"> 訪談資料庫主機連線對象、連線目的及使用之服務埠 實機檢視資料庫主機僅開啟允許之服務埠
	12	限制遠端存取來源	<ul style="list-style-type: none"> 訪談資料庫遠端存取控管機制 檢視資料庫遠端存取來源、連線授權紀錄，避免遭非授權來源 IP 進行連線

類別	項次	檢視項目	檢視要求
	13	限制遠端存取帳號	• 檢視資料庫遠端存取帳號與授權紀錄，避免遭非授權帳號進行遠端存取
	14	限制遠端存取操作	• 檢視資料庫遠端存取權限與授權紀錄，避免執行非授權之操作行為
	15	資料庫帳號權限最小原則	• 訪談資料庫身分識別、存取管理及權限劃分機制 • 檢視資料庫權限相關申請、審核紀錄，並實機檢視資料庫帳號權限遵循最小化原則
8.4 稽核紀錄	16	啟用資料庫帳號變更稽核	• 訪談資料庫稽核紀錄留存項目、保存期間及管理機制 • 實機檢視資料庫帳號異動稽核紀錄設定結果、留存內容及管理方式
	17	啟用資料庫帳號登出/登入稽核	• 實機檢視資料庫帳號登入/登出稽核紀錄設定結果、留存內容及管理方式
	18	啟用資料庫結構變更稽核	• 實機檢視資料庫結構異動稽核紀錄設定結果、留存內容及管理方式
	19	稽核紀錄管理方式	• 檢視資料庫稽核紀錄之存取控制與保存紀錄
	20	資料庫主機時間校時	• 訪談資料庫主機校時管理機制 • 實機檢視資料庫主機校時方式、來源及時間正確性
	21	稽核紀錄分析	• 訪談資料庫稽核紀錄分析機制及異常紀錄處理方式 • 實際檢視資料庫稽核紀錄分析規則設定、分析紀錄或報告，以及針對異常事件處理方式
8.5 委外管理	22	委外廠商外部連線方式	• 訪談資料庫委外廠商連線存取控管機制 • 檢視資料庫委外廠商外部連線方式設定、授權紀錄及相關防護機制
	23	委外廠商資料存取方式	• 檢視資料庫委外廠商資料存取方式、授權紀錄及相關防護機制
	24	委外廠商帳號授權方式	• 訪談資料庫委外廠商帳號權限管理機制 • 檢視資料庫委外廠商帳號權限設定、授權紀錄，確認帳號權限之適當性
8.6	25	資料庫定期執行	• 訪談資料庫備份管理機制

類別	項次	檢視項目	檢視要求
備份保護		備份	• 檢視資料庫備份方式(如備份時間、週期及方式等)與備份結果
	26	資料庫備份具有適當保護機制	• 訪談資料庫備份檔案之保護機制 • 檢視資料庫備份之存取控制與保護方式(包含異地儲存、內容加密、不可識別之處理等)
	27	資料庫備份回復測試	• 訪談資料庫備份回復測試執行方式 • 檢視資料庫備份回復測試演練執行結果與紀錄，確認演練之有效性
8.7 弱點管理	28	資料庫主機定期弱點掃描	• 訪談資料庫主機弱點掃描執行方式與頻率 • 檢視資料庫主機弱點掃描紀錄
	29	資料庫主機弱點修補	• 訪談資料庫主機弱點修補與追蹤機制 • 檢視資料庫主機弱點修補紀錄、相關審核紀錄及複測報告
	30	修補資料庫主機安全性更新項目	• 訪談資料庫與主機作業系統之安全性更新執行方式及頻率 • 實機檢視資料庫與主機作業系統之安全性更新歷程紀錄，確認是否已落實執行更新機制

(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*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)_網路設備紀錄檔分析	網路設備	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	
8.資料庫安全檢視	資料庫	5	1	1	5	
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 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)。

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、第 8 項為資料庫安全檢視，各服務項目採分項採購，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。

(三) 專案人員資格

1. 資安健診服務之專案人員資格(1~7 服務項目)，每位專案人員依各服務項目應具備專業證照如下：

(1) 網路架構檢視、防火牆連線設定檢視(服務項目 1、6)：需持有下列 1 張以上證照。

- 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。
- 其他網路安全相關專業證照。

(2) 網路(有線)、使用者端電腦、伺服器主機等惡意活動檢視(服務項目 2、3、4)：需持有下列 1 張以上證照。

- CEH(Certified Ethical Hacker)。
- CHFI(Computer Hacking Forensic Investigator)。
- CND(EC-Council Certified Network Defender)。
- SSCP(System Security Certified Practitioner)。
- CompTIA Security+。
- 其他網路、系統安全相關專業證照。

(3) 目錄伺服器設定檢視、政府組態基準(GCB)檢視(服務項目 5、服務項目 7)：需持有下列 1 張以上證照。

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。
- 其他系統安全相關專業證照。

2. 資料庫安全檢視(服務項目 8)：每位專案人員需持有下列 1 張以上證照，且團隊中須持有資料庫管理及資通安全技術/管理證照各 1 張以上。

(1) 資料庫管理：

- Azure Database Administrator Associate。
- Oracle Database Administration Certificated Professional。
- Oracle Certified Professional Oracle Database Security。
- IBM Certified Database Administrator。
- Certified MySQL Database Administrator (CMDDBA)。
- 其他資料庫相關專業證照。

(2) 資通安全技術/管理：

- CISSP(Certified Information Systems Security Professional)。
- ISO/CNS 27001 Lead Auditor。
- 其他資安技術/管理相關專業證照。

3. 為順利於履約前驗證專案人員資格條件，廠商應就上述資格條件先行確認符合規定，再檢附成員姓名、員工證明(如勞健保證明)、專業證照等影本，報請採購機關同意後始得服務。

4. 專案人員須年滿 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。

(四) 廠商應交付文件與辦理項目

1. 工作計畫書。
2. 資安健診服務報告。
3. 配合機關辦理至少 1 次說明會議。

(五) 交付文件說明

1. 工作計畫書

(1) 包含執行期間、執行項目、執行範圍、專案人員證照/年資/經歷、使用工具、執行方式、服務報告提交方式及相關執行資料之處理等。

(2) 佐證資料：專案人員資格證明(員工證明、專業證照文件)。

2. 資安健診服務報告

(1) 執行結果摘要說明(依照檢視項目分別摘要說明)。

(2) 執行計畫摘要

執行期間/執行項目/執行範圍/專案人員。

(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，說明其發生原因以及改善建議。

項目 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，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。

項目 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. 網路設備紀錄檔分析

依檢視之網路設備為序，表列包含設備名稱、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。

項目 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，依檢視之使用者電腦 IP 為序，分別說明檢視結果包含弱點說明、修補建議及發現之惡意程式檔名與改善建議。

3.2 使用者端電腦之作業系統、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。

- 3.3 檢視使用者端電腦是否使用已經終止支援之作業系統或軟體(如 Windows XP、Windows7、Office 2003、Office 2007、Adobe Flash Player 等，依使用作業系統或軟體之官網公告資訊為主)，針對使用終止支援之軟體，建議其停用並移除。

項目 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含弱點說明、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。
- 4.3 檢視伺服器是否使用已經終止支援之作業系統或軟體(如 Windows Server 2003、Office 2003、Office 2007、Adobe Flash Player 等，依使用作業系統或軟體之官網公告資訊為主)，針對使用終止支援之軟體，建議其停用並移除。
- 4.4 檢視伺服器是否使用不合宜之作業系統(如使用 Windows 7、Windows10 等)

項目 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。

項目 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。

項目 7 政府組態基準(GCB)檢視

- 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。

項目 8.資料庫安全檢視

- A.資料庫安全檢視 30 項整體摘要說明，詳列資料庫名稱、主機 IP、資料庫類型、版本，整體說明符合、不符合、部分符合、不適用之項目總數。
- B.詳細記錄每項檢測項目之檢視情形，除“符合、部分符合、不符合、不適用”勾選外，更要確實記錄每項檢視項目之機關現況與改善/建議事項，各項資料庫安全檢視結果判定原則及報告撰寫說明，詳見資料庫安全檢視結果判定原則及報告撰寫說明。

表2 資料庫安全檢視結果判定原則及報告撰寫說明

結果項目	符合 (勾選)	部分符合 (勾選)	不符合 (勾選)	不適用 (勾選)	檢視紀錄 內容	改善/建 議事項
判定原則 /撰寫說明	機關已訂 定管理機 制(若法 規有要求 須符合法 規要求) 且已落實 並保有紀 錄	<ul style="list-style-type: none"> •機關未 訂定管 理機 制，但 有實施 安控 •機關已 訂定管 理機 制，但 未完全 符合法 規要求 •機關已 訂定管 理機 制，但 未落實 實施 •機關已 訂定管 理機 制，已 落實但 無紀錄 	無任何管 理機制， 且無實施 安控與相 關紀錄	不適用	<ul style="list-style-type: none"> •記錄機 關現行 管理機 制(有文 件者， 記錄文 件名稱) •實機檢 視結果 •部分符 合、不 符合及 不適用 之情形 	<ul style="list-style-type: none"> •可再強 化之建 議 •不限定 哪一種 檢視結 果， (包含”符 合“，可 針對現行 機關管理 機制，提 出專業建 議，如機 關僅規定 修補高風 險弱點， 亦可視情 況給予中 低風險弱 點管理之 建議)

(4) 結果建議

說明目前資料庫整體防護情形及改善建議，包括制度規範強度、落實程度，加強措施及資源等。

(5) 結論

(6) 附件

A.側錄封包資料(燒錄至光碟或其他媒體裝置)。

B.服務紀錄檔(燒錄至光碟)

- C.發現惡意行為或惡意程式的過程紀錄與說明。
- D.使用者端電腦安全性未更新資訊。
- E.伺服器安全性未更新資訊。

(六) 廠商應配合及遵守事項

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。
3. 廠商於提供資安健診服務之前，須事先了解使用者端電腦與伺服器之官網公告，有關作業系統與軟體終止支援資訊。
4. 本案涉及資通訊軟體、硬體或服務等相關事務，廠商執行本案之團隊成員不得為陸籍人士，並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。

(七) 機關配合事項

1. 資安健診配合事項

- (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。

2. 資料庫安全檢視配合事項

- (1) 請安排 AP 管理者、DB 管理者及系統操作人員參與資料庫管理訪談，以供檢測人員可確實了解機關資料庫安全防護現況。
- (2) 請 DB 管理者備妥可查詢資料庫設定之帳號權限，於檢測過程協助相關操作。
- (3) 請備妥資料庫備份還原演練執行結果紀錄。
- (4) 資料庫主機弱點掃描報告與修補紀錄。

3. 若檢視之使用者端電腦、伺服器主機及資料庫，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)服務提供資通設備紀錄與資訊服務或應用程式紀錄等資安監控、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. SOC 監控範圍之整體處理效能總達 900 EPS(Event Per Second)，EPS 以 PEAK 或 MAX 值計算。
2. 監控 EPS 以日誌種類、設備數量推算所得，機關採購 SOC 服務前，須計算機關監控範圍之 EPS 需求，應納入「資通安全責任等級分級辦法」應辦事項之「資通安全防護」辦理項目、端點偵測及應變機制(EDR)、目錄服務系統及機關核心資通系統等之資通設備紀錄與資訊服務或應用程式紀錄。
3. 機關可參考過去 3 年監控上列項目之實際的 EPS，輔以表 1，作為採購 SOC 服務之參考。

表 1 日誌種類 EPS 參考表

序號	日誌種類	EPS
1	防毒軟體(防毒伺服器、防毒閘道器)	150
2	網路防火牆	300
3	郵件管理過濾機制	150
4	IDS	150
5	IPS	250
6	應用程式防火牆(WAF)	300
7	APT 防禦措施	150
8	網站主機	300
9	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

序號	日誌種類	EPS
13	檔案伺服器	150
14	資料庫伺服器	300
15	DNS 伺服器	150

(二) 計價方式

項目	單位	服務所需人天	SOC 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.情資回傳	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。人天費率為決標單價價格。

(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設備需求，廠商應與機關確認監控範圍已納入上述(一)2.SOC 監控範圍之相關設備與紀錄，經溝通後仍未納入監控範圍者，應於工作計畫書說明資安風險，以盡告知之義務，並完成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，檢視監控部署執行情形，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，對於同質或異質監控紀錄，透過 SIEM 或彙整機制進行整合，產生「資安監控單」。
- (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」，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)通知機關資安聯絡人，俾利機關進行情資處理。
- (3) 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、網頁形式等方式提交，而季報、年報則應到府進行提報。
- (4) 有關 SOC 監控回傳之相關規定，遵照資安法主管機關之要求辦理。

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
 - 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，了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. 情資回傳

依「資通安全責任等級分級辦法」第 11 條及附表一至附表四之規定，A、B 級公務機關及特定非公務機關應依規定完成資安威脅偵測管理機制建置，並持續維運，其中公務機關應依主管機關指定方式提交監控管理資料。

(1) 廠商應遵循國家資通安全研究院訂定之「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情資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。

配合廠商評鑑作業，將回傳能力、偵測能力及情資品質，列為監控成效分析指標，並納入廠商評鑑項目，做為評鑑監控有效性之參考。

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.有關「政府領域聯防監控作業規範」及相關表單，如「資安監控單」、「情資分析單」及「監控設備狀況單」等，

以國家資通安全研究院網站

(https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/N-SOC/)公告之資訊為主。

(2) 資安威脅預警

- A. 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：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 NICS、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。
- B. 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，內容包含資通安全威脅類型、說明、可能造成之影響、各大原廠發布的最新修正檔、新發現資通安全漏洞與補救措施、資通安全事件報導、漏洞分析、修補方式或對策。
- C. 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) 專案人員資格

1. 每位專案人員依各服務項目應具備專業證照如下：

(1) SOC 監控：需持有下列 1 張以上證照。

- CEH(EC-Council Certified Ethical Hacker)。
- CND(EC-Council Certified Network Defender)。
- CSA(EC-Council Certified SOC Analyst)。
- CTIA(EC-Council Certified Threat Intelligence Analyst)。
- CySA+(CompTIA Cybersecurity Analyst)。
- 其他資安相關專業證照。

(2) 資安事件處理：需持有下列 1 張以上證照。

- CEH(EC-Council Certified Ethical Hacker)。
- CHFI(EC-Council Computer Hacking Forensic Investigator)。
- CND(EC-Council Certified Network Defender)。
- ECIH(EC-Council Certified Incident Handler)。
- ECSA(EC-Council Certified Security Analyst)。
- 其他資安相關專業證照。

2. 為順利於履約前驗證專案人員資格條件，廠商應就上述資格條件先行確認符合規定，再檢附成員姓名、員工證明(如勞健保證明)、專業證照等影本，報請採購機關同意後始得服務。

3. 專案人員須年滿 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. 工作計畫書(包含監控環境部署建議)。
2. SOC 服務月報。
3. SOC 服務季報。
4. SOC 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. 工作計畫書

(1) 基本資訊：執行期間/執行項目/執行範圍/專案人員(資安年資/證照資訊)。

- (2) 執行規劃：包含各項工作執行規劃、監控設備部署規劃、監控、情資回傳及警示作業之方式、通知機關資安聯絡人之時機、內容及方式、資安事件處理作業、資安威脅預警作業等。
- (3) 風險說明：廠商應協助機關盤整資安法要求之監控範圍(上述(一)2.之項目)，對於未納入監控者，應列出资安風險，盡告知之義務。
- (4) 各項報告(月報、季報、年報)提交時間及內容。
- (5) 佐證資料：專案人員資格證明(員工證明、專業證照文件)。

2. SOC 服務月報

- (1) 資安監控與情資回傳分析，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。交付文件必須包含指定欄位內容，呈現方式形式不拘。
 - 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；另依據「政府領域聯防監控作業規範」要求欄位，詳列「情資分析單」內容。
 - 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，彙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。
- (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，包含資通安全威脅類型、說明、可能造成之影響、各大原廠發布的最新修正檔、新發現資通安全漏洞與補救措施、資通安全事件報導、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 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，包含：

(1) 監控與情資回傳分析

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. 當季資安監控情資統計，包含事件主旨、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，清楚當季外部威脅連線 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，檢視監控部署執行情形，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 服務年報

(1) 資安監控與情資回傳分析

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，彙整近 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記錄，並提出矯正預防措施建議，包含精進內部程序文件、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，包含事件編號、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，包含資料蒐集、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) 廠商應遵守事項

本案涉及資通訊軟體、硬體或服務等相關事務，廠商執行本案之團隊成員不得為陸籍人士，並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。

(八) 機關配合事項

1. 機關應提供適當環境配合 SOC 監控環境部署。
2. 機關應提供資通設備清單與核心資通系統清單。

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)服務提供資通設備紀錄與資訊服務或應用程式紀錄等資安監控、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. SOC 監控範圍之整體處理效能總達 2,300 EPS(Event Per Second)，EPS 以 PEAK 或 MAX 值計算。
2. 監控 EPS 以日誌種類、設備數量推算所得，機關訂購 SOC 服務前，須計算機關監控範圍之 EPS 需求，應納入「資通安全責任等級分級辦法」應辦事項之「資通安全防護」辦理項目、端點偵測及應變機制(EDR)、目錄服務系統及機關核心資通系統等之資通設備紀錄與資訊服務或應用程式紀錄。
3. 機關可參考過去 3 年監控上列項目之實際的 EPS，輔以下表 1，作為採購 SOC 服務之參考。

表 1 日誌種類 EPS 參考表

序號	日誌種類	EPS
1	防毒軟體(防毒伺服器、防毒閘道器)	150
2	網路防火牆	300
3	郵件管理過濾機制	150
4	IDS	150
5	IPS	250
6	應用程式防火牆(WAF)	300
7	APT 防禦措施	150
8	網站主機	300
9	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

序號	日誌種類	EPS
13	檔案伺服器	150
14	資料庫伺服器	300
15	DNS 伺服器	150

(二) 計價方式

項目	單位	服務所需人天	SOC 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. 情資回傳	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。人天費率為決標單價價格。

(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設備需求，廠商應與機關確認監控範圍已納入上述(一)2.SOC 監控範圍之相關設備與紀錄，經溝通後仍未納入監控範圍者，應於工作計畫書說明資安風險，以盡告知之義務，並完成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，檢視監控部署執行情形，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 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，對於同質或異質監控紀錄，透過 SIEM 或彙整機制進行整合，產生「資安監控單」。
- (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」，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)通知機關資安聯絡人，俾利機關進行情資處理。
- (3) 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。
- (4) 有關 SOC 監控回傳之相關規定，遵照資安法主管機關之要求辦理。

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，了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. 情資回傳

依「資通安全責任等級分級辦法」第 11 條及附表一至附表四之規定，A、B 級公務機關及特定非公務機關應依規定完成資安威脅偵測管理機制建置，並持續維運，其中公務機關應依主管機關指定方式提交監控管理資料。

(1) 廠商應遵循國家資通安全研究院訂定之「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情資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。

配合廠商評鑑作業，將回傳能力、偵測能力及情資品質，列為監控成效分析指標，並納入廠商評鑑項目，做為評鑑監控有效性之參考。

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 監控情資回傳作業。

E.有關「政府領域聯防監控作業規範」及相關表單，如「資安監控單」、「情資分析單」及「監控設備狀況單」等，以國家資通安全研究院網站

(https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/N-SOC/) 國家資安聯防監控中心(N-SOC)公告之資訊為主。

(2) 資安威脅預警

- A. 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：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 NICS、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。
- B. 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，內容包含資通安全威脅類型、說明、可能造成之影響、各大原廠發布的最新修正檔、新發現資通安全漏洞與補救措施、資通安全事件報導、漏洞分析、修補方式或對策。
- C. 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) 專案人員資格

1. 每位專案人員依各服務項目應具備專業證照如下：

(1) SOC 監控：需持有下列 1 張以上證照

- CEH(EC-Council Certified Ethical Hacker)。
- CND(EC-Council Certified Network Defender)。
- CSA(EC-Council Certified SOC Analyst)。
- CTIA(EC-Council Certified Threat Intelligence Analyst)。
- CySA+(CompTIA Cybersecurity Analyst)。
- 其他資安相關專業證照。

(2) 資安事件處理：需持有下列 1 張以上證照

- CEH(EC-Council Certified Ethical Hacker)。
- CHFI(EC-Council Computer Hacking Forensic Investigator)。
- CND(EC-Council Certified Network Defender)。
- ECIH(EC-Council Certified Incident Handler)。
- ECSA(EC-Council Certified Security Analyst)。
- 其他資安相關專業證照。

2. 為順利於履約前驗證專案人員資格條件，廠商應就上述資格條件先行確認符合規定，再檢附成員姓名、員工證明(如勞健保證明)、專業證照等影本，報請採購機關同意後始得服務。

3. 專案人員須年滿 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. 工作計畫書(含 SOC 監控環境部署建議)。
2. SOC 服務月報。
3. SOC 服務季報。
4. SOC 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. 工作計畫書

(1) 基本資訊：執行期間、執行項目、執行範圍、專案人員證照/年資/經歷。

- (2) 執行規劃：包含各項工作執行規劃、監控設備部署規劃、監控、情資回傳及警示作業之方式、通知機關資安聯絡人之時機、內容及方式、資安事件處理作業、資安威脅預警作業等。
- (3) 風險說明：廠商應協助機關盤整資安法要求之監控範圍(上述(一)2.之項目)，對於未納入監控者，應列出资安風險，盡告知之義務。
- (4) 各項報告(月報、季報、年報)提交時間及內容。
- (5) 佐證資料：專案人員資格證明(員工證明、專業證照文件)。

2. SOC 服務月報

- (1) 資安監控與情資回傳分析，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。交付文件必須包含指定欄位內容，呈現方式形式不拘。
 - 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；另依據「政府領域聯防監控作業規範」要求欄位，詳列「情資分析單」內容。。
 - 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，清楚當月外部威脅連線 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，包含資通安全威脅類型、說明、可能造成之影響、各大原廠發布的最新修正檔、新發

現資通安全漏洞與補救措施、資通安全事件報導、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 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，包含：

(1) 資安監控與情資回傳分析

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. 當季資安監控情資統計，包含事件主旨、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，清楚當季外部威脅連線 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，檢視監控部署執行情形，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 服務年報

(1) 資安監控與情資回傳分析

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記錄，並提出矯正預防措施建議，包含精進內部程序文件、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，包含事件編號、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，包含資料蒐集、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) 廠商應遵守事項

本案涉及資通訊軟體、硬體或服務等相關事務，廠商執行本案之團隊成員不得為陸籍人士，並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。

(八) 機關配合事項

1. 機關應提供適當環境配合 SOC 監控環境部署。
2. 機關應提供資通設備清單與核心資通系統清單。

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)服務提供資通設備紀錄與資訊服務或應用程式紀錄等資安監控、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. SOC 監控範圍之整體處理效能總達 4,900 EPS(Event Per Second)，EPS 以 PEAK 或 MAX 值計算。
2. 監控 EPS 以日誌種類、設備數量推算所得，機關採購 SOC 服務前，須計算機關監控範圍之 EPS 需求，應納入「資通安全責任等級分級辦法」應辦事項之「資通安全防護」辦理項目、端點偵測及應變機制(EDR)、目錄服務系統及機關核心資通系統等之資通設備紀錄與資訊服務或應用程式紀錄。
3. 機關可參考過去 3 年之監控上列項目之實際的 EPS，輔以表 1，作為採購 SOC 服務之參考。

表 1 日誌種類 EPS 參考表

序號	日誌種類	EPS
1	防毒軟體(防毒伺服器、防毒閘道器)	150
2	網路防火牆	300
3	郵件管理過濾機制	150
4	IDS	150
5	IPS	250
6	應用程式防火牆(WAF)	300
7	APT 防禦措施	150
8	網站主機	300
9	路由器	250
10	代理伺服器	250
11	郵件伺服器	200

序號	日誌種類	EPS
12	目錄伺服器	150
13	檔案伺服器	150
14	資料庫伺服器	300
15	DNS 伺服器	150

(二) 計價方式

項目	單位	服務所需人天	SOC 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. 情資回傳	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。人天費率為決標單價價格。

(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設備需求，廠商應與機關確認監控範圍已納入上述(一)2.SOC 監控範圍之相關設備與紀錄，經溝通後仍未納入監控範圍者，應於工作計畫書說明資安風險，以盡告知之義務，並完成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，檢視監控部署執行情形，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，對於同質或異質監控紀錄，透過 SIEM 或彙整機制進行整合，產生「資安監控單」。
- (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」，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)通知機關資安聯絡人，俾利機關進行情資處理。
- (3) 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。
- (4) 有關 SOC 監控回傳之相關規定，遵照資安法主管機關之要求辦理。

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
 - 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，了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. 情資回傳

依「資通安全責任等級分級辦法」第 11 條及附表一至附表四之規定，A、B 級公務機關及特定非公務機關應依規定完成資安威脅偵測管理機制建置，並持續維運，其中公務機關應依主管機關指定方式提交監控管理資料。

(1) 廠商應遵循國家資通安全研究院訂定之「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情資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。

配合廠商評鑑作業，將回傳能力、偵測能力及情資品質，列為監控成效分析指標，並納入廠商評鑑項目，做為評鑑監控有效性之參考。

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.有關「政府領域聯防監控作業規範」及相關表單，如「資安監控單」、「情資分析單」及「監控設備狀況單」等，

以國家資通安全研究院網站

(https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/N-SOC/)公告之資訊為主。

(2) 資安威脅預警

- A. 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：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 NICS、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。
- B. 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，內容包含資通安全威脅類型、說明、可能造成之影響、各大原廠發布的最新修正檔、新發現資通安全漏洞與補救措施、資通安全事件報導、漏洞分析、修補方式或對策。
- C. 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) 專案人員資格

1. 每位專案人員依各服務項目應具備專業證照如下：

(1) SOC 監控：需持有下列 1 張以上證照

- CEH(EC-Council Certified Ethical Hacker)。
- CND(EC-Council Certified Network Defender)。
- CSA(EC-Council Certified SOC Analyst)。
- CTIA(EC-Council Certified Threat Intelligence Analyst)。
- CySA+(CompTIA Cybersecurity Analyst)。
- 其他資安相關專業證照。

(2) 資安事件處理：需持有下列 1 張以上證照

- CEH(EC-Council Certified Ethical Hacker)。
- CHFI(EC-Council Computer Hacking Forensic Investigator)。
- CND(EC-Council Certified Network Defender)。
- ECIH(EC-Council Certified Incident Handler)。
- ECSA(EC-Council Certified Security Analyst)。
- 其他資安相關專業證照。

2. 為順利於履約前驗證專案人員資格條件，廠商應就上述資格條件先行確認符合規定，再檢附成員姓名、員工證明(如勞健保證明)、專業證照等影本，報請採購機關同意後始得服務。

3. 專案人員須年滿 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. 工作計畫書(含 SOC 監控環境部署建議)。
2. SOC 服務月報。
3. SOC 服務季報。
4. SOC 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. 工作計畫書

(1) 基本資訊：執行期間、執行項目、執行範圍、專案人員證照/年資/經歷。

- (2) 執行規劃：包含各項工作執行規劃、監控設備部署規劃、監控、情資回傳及警示作業之方式、通知機關資安聯絡人之時機、內容及方式、資安事件處理作業、資安威脅預警作業等。
- (3) 風險說明：廠商應協助機關盤整資安法要求之監控範圍(上述(一)2.之項目)，對於未納入監控者，應列出资安風險，以盡告知之義務。
- (4) 各項報告(月報、季報、年報)提交時間及內容。
- (5) 佐證資料：專案人員資格證明(員工證明、專業證照文件)。

2. SOC 服務月報

- (1) 資安監控與情資回傳分析，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。交付文件必須包含指定欄位內容，呈現方式形式不拘。
 - 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；另依據「政府領域聯防監控作業規範」要求欄位，詳列「情資分析單」內容。。
 - 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，清楚當月外部威脅連線 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，包含資通安全威脅類型、說明、可能造成之影響、各大原廠發布的最新修正檔、新發

現資通安全漏洞與補救措施、資通安全事件報導、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 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，包含：

(1) 資安監控與情資回傳分析

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. 當季資安監控情資統計，包含事件主旨、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，清楚當季外部威脅連線 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，檢視監控部署執行情形，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 服務年報

(1) 資安監控與情資回傳分析

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記錄，並提出矯正預防措施建議，包含精進內部程序文件、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，包含事件編號、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，包含資料蒐集、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) 廠商應遵守事項

本案涉及資通訊軟體、硬體或服務等相關事務，廠商執行本案之團隊成員不得為陸籍人士，並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。

(八) 機關配合事項

1. 機關應提供適當環境配合 SOC 監控環境部署。
2. 機關應提供資通設備清單與核心資通系統清單。

三、第 3 組弱點掃描服務

弱點掃描服務提供主機系統弱點掃描、Web 網頁弱點掃描及網頁個資掃描等項目，透過弱點掃描作業協助機關發現安全弱點或個資揭露，提供弱點掃描結果與弱點修補建議，並於協助修補弱點後提供複測，以確認已經完成修正。

(一) 服務說明

1. 服務項目：分為主機系統弱點掃描、Web 網頁弱點掃描及網頁個資掃描。

(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掃描，系統弱點掃描的項目，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掃描。
- G. 網路通訊埠掃描。

(2) Web 網頁弱點掃描

針對機關網頁安全弱點進行掃描，掃描項目應符合 OWASP TOP 10 項目(以官方網站公告最新資訊為主，請廠商以最新內容掃描)。

(3) 網頁個資掃描

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掃描，掃描個資特徵應至少包含中文姓名、地址、電話(含市話/手機)、電子郵件信箱、中華民國身分證字號、健保卡號、護照號碼及信用卡號等個人資料掃描。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，並提醒機關檢視個資揭露之合宜性。

2. 掃描次數

於訂購後半年內，依機關採購項目提供以下服務次數：

服務項目	次數
主機系統弱點掃描	2 次掃描(初掃、複掃)
Web 網頁弱點掃描	2 次掃描(初掃、複掃)
網頁個資掃描	1 次掃描

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。

(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 ($\frac{\text{服務所需人天}}{\text{採購數量}}$)	單項服務金額 (採購數量所需人天*人天費率)
1	主機系統弱點掃描-到場服務	IP	0.35	15	0	0	
2	主機系統弱點掃描-遠端服務	IP	0.3	10	100	30	
3	WEB 網頁弱點掃描(WebVA)-到場服務	URL	3	1	0	0	
4	WEB 網頁弱點掃描(WebVA)-遠端服務	URL	2	1	10	20	
5	網頁個資掃描-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)。

計價方式說明：

1. 弱點掃描服務，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。

(三) 專案人員資格

1. 每位專案人員應具備專業要求，需持有下列 1 張以上證照。
 - CEH(EC-Council Certified Ethical Hacker)。
 - CPENT(EC-Council Certified Penetration Tester)。
 - CompTIA PenTest+。
 - CPSA(The CREST Practitioner Security Analyst)。
 - OSCP(Offensive Security Certified Professional)。
 - 其他資安相關專業證照。
2. 為順利於履約前驗證專案人員資格條件，廠商應就上述資格條件先行確認符合規定，再檢附成員姓名、員工證明(如勞健保證明)、專業證照等影本，報請採購機關同意後始得服務。
3. 專案人員須年滿 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。

(四) 廠商應交付文件及辦理項目

1. 工作計畫書。
2. 弱點掃描服務中文報告(初掃與複掃均應提供)。
3. 配合機關初掃與複掃原則上各辦理 1 次說明會議(視機關需求)。

(五) 交付文件說明

1. 工作計畫書
 - (1) 包含執行期間、執行項目、執行範圍、專案人員證照/年資/經歷、使用工具、執行方式、服務報告提交方式及相關執行資料之處理等。
 - (2) 佐證資料：專案人員資格證明(員工證明、專業證照文件)。
2. 弱點掃描服務中文報告(初掃與複掃)

(1) 執行結果摘要說明。

(2) 執行計畫摘要說明

執行期間/執行項目/執行範圍/專案人員。

(3) 執行情形

A. 整體結果統計說明。

B. 掃描時間、掃描方式、掃描工具說明。

C. 弱點發現及改善建議：針對各項掃描結果，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掃描使用者電腦 IP，以利機關了解弱點可能造成之影響並進行修補與追蹤。

D. 網頁個資掃描情形：針對網站之內容進行個人資料之特徵資訊掃描，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。

(六) 廠商應遵守事項

本案涉及資通訊軟體、硬體或服務等相關事務，廠商執行本案之團隊成員不得為陸籍人士，並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。

(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。

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：門禁系統、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	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、Code Injection、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
	網站服務套件	包含常見 WEB 套件弱點測試，如設定缺

測試類型	測試類別	測試項目
		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
	其他	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掃描項目
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

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

測試類型	測試類別	測試項目
	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
應用程式	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
	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
	其他	包含 SMB、LPD、IPP、Jetdirect、SNMP 及 RTSP 等常見應用程式或網路套件之弱點掃描項目
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. 物聯網設備配套滲透測試參考

項次	物聯網設備類型	設備類型檢測範圍
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	門禁系統	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 etc

6	網路儲存裝置 (NAS)	網路儲存裝置
7	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-到場服務	URL 或 IP	16	1	1	16	
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）。

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。

(三) 專案人員資格

1. 每位專案人員應具備專業要求，需持有下列 1 張以上證照。

➤ CEH(EC-Council Certified Ethical Hacker)。

- CPENT(EC-Council Certified Penetration Tester)。
- CompTIA PenTest+。
- CPSA(The CREST Practitioner Security Analyst)。
- OSCP(Offensive Security Certified Professional)。
- 其他資安相關專業證照。

2. 為順利於履約前驗證專案人員資格條件，廠商應就上述資格條件先行確認符合規定，再檢附成員姓名、員工證明(如勞健保證明)、專業證照等影本，報請採購機關同意後始得服務。
3. 專案人員須年滿 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。

(四) 廠商應交付文件及辦理項目

1. 工作計畫書。
2. 滲透測試服務報告(初測與複測均應提供)。
3. 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)。

(五) 交付文件說明

1. 工作計畫書

- (1) 包含執行期間、執行項目、執行範圍、專案人員證照/年資/經歷、使用工具、執行方式、服務報告提交方式及相關執行資料之處理等。
- (2) 佐證資料：專案人員資格證明(員工證明、專業證照文件)。

2. 滲透測試服務報告(初測與複測)

(1) 執行計畫摘要

執行期間/執行項目/執行範圍/專案人員。

(2) 執行結果摘要說明

- A. 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)。
- B. 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)。
- C. 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(包含檢測目標/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。

A. 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。

B. 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。

(六) 廠商應遵守事項

本案涉及資通訊軟體、硬體或服務等相關事務，廠商執行本案之團隊成員不得為陸籍人士，並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。

(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

社交工程演練服務包含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了解社交工程的存在，並提高警覺性；同時受測機關可以根據測試結果瞭了解可能發生安全缺口，藉以實施其內部教育訓練來補強，並作為資通安全的管理依據。

(一) 服務說明

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	<ol style="list-style-type: none"> 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，包含本文、附件、可連結資訊。 	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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「社交工程郵件開啟」及「社交工程郵件點閱」等受測者行為。 	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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「社交工程郵件開啟」及「社交工程郵件點閱」等受測者行為。(須先排除非 	<ol style="list-style-type: none"> 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率」等結果。

服務項目/服務內容	1.電子郵件測試服務	2.簡訊測試服務
	<p>人為觸發之行為)</p> <p>4. 受測者開啟與點閱細部時間紀錄。</p> <p>5. 統計「社交工程郵件開啟率」及「社交工程郵件點閱率」等結果。</p> <p>6. 社交工程郵件觸發統計基準說明：</p> <p>(1)社交工程郵件開啟率：開啟社交工程郵件之人數／參演人數。</p> <p>(2)社交工程郵件點閱率：點閱社交工程郵件所附連結或檔案之人數／參演人數。</p>	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	

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)
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 (201~500)	13 (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)。

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。

(三) 專案人員資格

1. 每位專案人員應具備專業要求，需持有下列 1 張以上證照。

- CEH(Certified Ethical Hacker)。
- CND(EC-Council Certified Network Defender)。

- CompTIA Security+。
- ECIH(EC-Council Certified Incident Handler Course)。
- iPAS 資訊安全工程師中級能力鑑定。
- 其他資安相關專業證照。

2. 為順利於履約前驗證專案人員資格條件，廠商應就上述資格條件先行確認符合規定，再檢附成員姓名、員工證明(如勞健保證明)、專業證照等影本，報請採購機關同意後始得服務。
3. 專案人員須年滿 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。

(四) 廠商應交付項目及配合事項

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

(五) 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國家資通安全研究院，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情形。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，包含：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@nics.nat.gov.tw;

(1) 郵件主旨如下：

主旨：〔廠商名稱〕共契服務_113 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：113/11/1 迄：113/12/01	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。

(六) 交付文件說明

1. 工作計畫書

(1) 包含執行期間、執行項目、執行範圍、專案人員證照/年資/經歷、使用工具、執行方式、服務報告提交方式及相關執行資料之處理等。

(2) 佐證資料：專案人員資格證明(員工證明、專業證照文件)。

2. 社交工程演練服務_電子郵件/簡訊測試報告

(1) 執行結果摘要說明。

(2) 執行計畫摘要

執行期間/執行項目/執行範圍/專案人員。

(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	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	2. 簡訊派送時間表
3. 統計「社交工程郵件開啟」、「社交工程郵件點閱」等受測者行為(須先排除非人為觸發之行為)	3. 統計「點閱簡訊內容之連結」之受測者行為
4. 統計「社交工程郵件開啟率」、「社交工程郵件點閱率」等結果	4. 統計「點閱簡訊內容之連結率」之結果
5. 受測者開啟與點閱細部時間紀錄	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。

(七) 廠商應遵守事項

本案涉及資通訊軟體、硬體或服務等相關事務，廠商執行本案之團隊成員不得為陸籍人士，並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。

(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通安全的管理依據。

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至少 4 次到場計劃性維護服務，並協助進行防火牆日常設定、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畫，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，惟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通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：通過 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，機關須配合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。

七、第 7 組 紅隊演練服務 (本次新增)

為能提升機關(構)之資通安全防護能力並找出潛藏於機關(構)營運之重大資安風險，擬透過第三方廠商進行紅隊演練服務，以攻擊者或白帽駭客之攻擊戰術、技術及程序(Tactics, Techniques, Procedures, TTPs)，在有限時間內且不影響系統運作前提下，利用攻擊手法以達成指定目標，並經由演練結果檢視現有防禦設備之有效性、管理制度及程序的落實性、監控範圍之合理性及反應時間之適切性。

(一)服務範圍(演練範圍)

為採購機關(構)所有人員與擁有之資訊資產(即支援[資訊](#)相關活動所需之資產)，包含：

- 1.實體資產：如機房、辦公室、資料中心等。
- 2.硬體資產：如伺服器、路由器(Router)、無線存取點(Wireless Access Point)、入侵防護設備(IPS)、防火牆(Firewall)及相關物聯網設備等。
- 3.軟體資產：如作業系統、套裝軟體、自行或委外開發之應用程式及資通系統(包含雲端與地端系統)等。
- 4.資訊：如數位與紙本資訊。
- 5.人員：如正式員工、約聘僱人員及委外人力等。
- 6.採購機關(構)指定之網域或 IP。

(二)服務目標(演練目標)

1.取得至少 1 個機關(構)指定之控制權(依機關需求定義)，如：

(1)資通系統：如核心資通系統、目錄服務系統(Active Directory Domain Services, AD)等資通系統。

(2)資通安全防護措施：如防火牆、入侵偵測系統(Intrusion Detection System,

IDS)、防毒軟體等措施。

- 2.取得至少 1 項機關(構)指定之資訊類資訊資產(依機關需求定義)，如機密文書、個人資料、程式原始碼等。
- 3.其他建議之適切目標：於演練過程中，雙方視情況得異動演練目標，且經雙方同意後執行。

(三)服務工作項目說明

- 1.廠商應於機關(構)訂購單通知之次工作日起算 30 個日曆天內，勘查採購機關(構)之演練範圍，針對整體安全進行評估，並撰寫「紅隊演練服務工作計畫書」，採擬真方式以駭客思維入侵並達到演練目標，以檢視演練範圍營運上可能存在之資安風險，並檢視演練範圍防禦機制，持續改善資安防護之能力。
- 2.演練方式：在一般人員未知情況下在指定演練範圍，至少須進行外網入侵、內網入侵演練情境，演練目標依採購機關(構)之防禦機制(藍隊)採取監控不阻擋或監控並阻擋方式進行。相關演練情境可參考國家資通安全研究院官網公布(<https://www.nics.nat.gov.tw>) 之資安資源/參考文件/共通規範之紅隊演練作業參考指引。
- 3.演練攻擊方式可參考最新 MITRE 之 ATT&CK 框架，演練作業流程可分為偵察([Reconnaissance](#))、資源開發([Resource Development](#))、初始存取([Initial Access](#))、執行([Execution](#))、持續([Persistence](#))、提權([Privilege Escalation](#))、避免偵測([Defense Evasion](#))、憑證存取([Credential Access](#))、發現([Discovery](#))、橫向移動([Lateral Movement](#))、蒐集([Collection](#))、命令與控制([Command and Control](#))、滲漏([Exfiltration](#))及影響([Impact](#))等 14 種網路攻擊戰術與 234 種技術(數字以最新公告為主)，廠商可依照受測範圍與演練情境彈性選擇相關應用，並於紅隊演練服務工作計畫書之紅隊演練計畫說明預計使用之演練戰術。
- 4.於訂購後半年內，執行紅隊演練初測與複測各 1 次。

- 5.紅隊演練初測執行時程至少 4 週，另針對初測服務作業發現弱點，廠商應納入紅隊演練服務初測報告，並提供修補建議。
- 6.於複測服務作業時，廠商應視機關需求，驗測初測作業所發現弱點，並於複測服務報告中說明機關之改善情形。
- 7.廠商應於演練期間每日製作工作日誌，日誌中應詳實記錄工作軌跡紀錄，如入侵時序、途徑、相關異動資訊等，並彙整於最後演練報告中說明。
- 8.廠商於演練過程中如發現重大漏洞時，應立即通知採購機關(構)並提供修補建議；其餘風險則於演練報告中呈現。
- 9.紅隊攻擊者在過程如攻擊行為可能影響演練機關(構)業務正常運作時，應先行與演練機關(構)確認，獲得同意後方可執行。
- 10.廠商於檢測完畢後須協助機關還原系統環境及清除相關異動(含帳號、資料及工具程式等)。
- 11.廠商於演練作業屆期前已達成服務目標(演練目標)，仍應於演練作業時程內，持續嘗試挖掘並以其他入侵路徑等方式提供演練服務，協助機關發掘潛在弱點，不以達成服務目標 (演練目標)為由而停止演練；倘廠商利用各種演練攻擊方式仍未能達成服務目標(演練目標)者，亦應於報告中舉證證明執行過程之攻擊手法與結果，且說明機關之防護措施成功阻擋狀況；針對上述情形，廠商應完整紀錄於演練日誌，並於報告中呈現。
- 12.廠商須配合出席採購機關要求之相關會議，如說明會、專案會議等。

(四)計價方式

項目	單位
----	----

項目	單位
1. 執行服務(演練)目標之演練工作 2. 完成交付文件 (1)紅隊演練服務工作計畫書(含演練計畫) (2)紅隊演練服務初測報告 (3)紅隊演練服務複測報告	乙式

註：上列項目視為乙式服務(報價標的)，以總價報價。

(五)專案人員資格

- 1.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。
- 2.專案人員由多數人組成，其中至少 1 位專案負責人與 3 位紅隊演練檢測人員。
- 3.紅隊演練檢測人員應具備以下專業要求以確保服務水準，並於建議書中檢附成員姓名、員工證明(如勞健保證明)、專業證照、專業經驗證明與特殊經歷證明等文件影本以供審核。
- 4.紅隊演練檢測人員須經機關同意始可參與。
- 5.紅隊演練檢測人員，專業資格要求：(皆須符合條件)
 - (1)團隊之每位紅隊演練檢測人員須具備滲透測試、紅隊演練或漏洞挖掘相關經驗不得少於 3 年。
 - (2)團隊之紅隊演練檢測人員中，至少 3 位各自具備 1 張實戰實機(hand-on)考試之證照。證照如：(原則依字母順序排序)
 - CBBH(HTB Certified Bug Bounty Hunter)。
 - CWEE(HTB Certified Web Exploitation Expert)。
 - CPTS(HTB Certified Penetration Testing Specialist)。

- CRTE(Altered Security Certified Red Team Expert)。
- CRTM(Altered Security Certified Red Team Master)。
- CRTP(Altered Security Certified Red Team Professional)。
- CRTO(Zero-Point Security Certified Red Team Operator)。
- eCPPT(INE Security Certified Professional Penetration Tester)。
- eWPT(INE Security eLearnSecurity Web Application Penetration Tester)。
- eWPTX(INE Security Web application Penetration Tester eXtreme)。
- LPT(EC-Council Licensed Penetration Testing)。
- OSCE³(OSWE+OSEP+OSED)。
- OSCP(Offensive Security Certified Professional)。
- OSED(Offensive Security Exploit Development)。
- OSEE(Offensive Security Advanced Windows Exploitation)。
- OSEP(Offensive Security Experienced Penetration Tester)。
- OSWE(Offensive Security Web Expert)。
- PNPT(TCM Security Practical Network Penetration Tester)。
- 其他資安相關實戰實機專業證照(需經採購機關(構)核可)。

(3)團隊之紅隊演練檢測人員中，至少 1 人符合下列特殊經歷至少 1 項。

- 具備尋找零時差漏洞之能力與實績(如有挖掘國際知名產品 CVE 弱點之證明或佐證)。
- 近 3 年至少須有 1 位成員曾參與國際 CTF 比賽與獲取實績，如 DEFCON CTF、Plaid CTF、Boston Key Party CTF 等。

- － 具備弱點研究能力，曾於國際知名研討會發表研究成果(如 HITCON、Black Hat、DEF CON、CODE BLUE、CODEGATE、HITB 等)。
- － 曾參與國際企業 Bug Bounty 計畫且獲得獎勵。
- － 其他資安相關專業經歷(需經採購機關(構)核可)。

(六)交付項目與時程

項次	交付項目	交付內容	數量	交付型態	交付期限
1	紅隊演練服務工作計畫書(含演練計畫)(中文)	文件內容： <ul style="list-style-type: none"> ▪ 專案簡介 ▪ 演練目標與範圍 ▪ 專案人員證照/年資/經歷 ▪ 準備與資源 ▪ 專案整體時程(包含初測及複測時間等規劃) ▪ 紅隊演練計畫 ▪ 演練執行(包含演練情境、演練攻擊戰術等) ▪ 事後分析與報告 ▪ 演練評估與改進 ▪ 相關執行資料之處理等 ▪ 佐證資料：專案人員資格證明(員工證明、紅隊演練檢測人員之專業證照、特殊經歷證明等文件) 	乙份	電子檔\紙本	接收機關(構)訂購單通知之次工作日起算30個日曆天內交付

項次	交付項目	交付內容	數量	交付型態	交付期限
2	紅隊演練服務初測報告 (中文)	文件內容： <ul style="list-style-type: none"> ▪ 演練期間 ▪ 服務人員 ▪ 演練過程所使用之技術與工具說明 ▪ 全案需詳細記錄弱點細節，包含風險等級、弱點位置、弱點描述、圖示、修補建議 ▪ 演練結果統計 ▪ 演練效益說明 ▪ 檢討及建議 ▪ 工作日誌(演練相關佐證與軌跡紀錄，如入侵時序、途徑、相關異動資訊等) 	乙份	電子檔\紙本	紅隊演練初測完成次一日曆天起 20 個日曆天內交付
3	紅隊演練服務複測報告 (中文)	文件內容： <ul style="list-style-type: none"> ▪ 演練期間 ▪ 服務人員 ▪ 演練過程所使用之技術與工具說明 ▪ 全案需詳細記錄弱點細節，包含風險等級、弱點位置、弱點描述、圖示、修補建議 ▪ 演練結果統計 ▪ 演練效益說明 ▪ 檢討及建議 	乙份	電子檔\紙本	紅隊演練複測完成次一日曆天起 20 個日曆天內交付

項次	交付項目	交付內容	數量	交付型態	交付期限
		<ul style="list-style-type: none"> 工作日誌(演練相關佐證與軌跡紀錄，如入侵時序、途徑、相關異動資訊等) 			

(七)服務水準協定(SLA)

廠商於履行契約期間，履約品質應依照本案各項服務水準協定，以應達成之工作服務項目要求為依據，並透過客觀之證據或指標，辦理自主檢查，做為品質管制，但廠商有承諾較高之服務水準時，應從其承諾：

項次	項目	服務水準
1	執行時程	<ul style="list-style-type: none"> 初測：1 次，至少 4 週 複測：1 次
2	交付文件	<ul style="list-style-type: none"> 紅隊演練服務工作計畫書(含演練計畫) 紅隊演練服務初測報告 紅隊演練服務複測報告 依指定時間、內容要求提供。
3	日誌交付	廠商應於檢測期間應每日製作工作日誌，並於隔日交付機關，日誌中應詳實記錄工作軌跡紀錄
4	重大漏洞通報	廠商於檢測過程中如發現重大漏洞，應立即通知機關即時修補
5	清除相關異動	廠商於檢測完畢後須協助機關還原系統環境及清除相關異動(含帳號、資料及工具程式等)

(八)廠商應遵守事項

本案涉及資通訊軟體、硬體或服務等相關事務，廠商執行本案之團隊成員不得為陸籍人士，並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(構)利用服務之所屬一切資料存取、傳輸、備份、及備援之實體所在地，應為我國管轄權所及之境內。

(九)機關(構)配合事項

執行作業時間由機關(構)與廠商協調取得適當時間進行。