採購規格書

壹、設備規格

一、內網資安政策自動化符規偵測器硬體規格

(一)、硬體式偵測器須具備以下功能

1. 採硬體式設備(Hardware Appliance)架構，且為 Linux Kernel 作業系統，故障時可以同型式設備直接替換。
2. 提供本會中部及南部辦公室共 2 臺(含)以上，每臺效能可同時收集 100 個以上端點設備及具備 IEEE 802.1Q 標準 Trunk 之 Multiple VLAN 的管控設備。(可由產品型錄證明)
3. 提供本會內湖 B 棟共 1 臺(含)以上，每臺效能可同時收集 5000 個以上端點設備及具備 IEEE 802.1Q 標準 Trunk 之 Multiple VLAN 的管控設備。(可由產品型錄證明)

(二)、具備提供自訂離線政策保留時間，當探測器與內網資安政策符規覆核平台離線仍可持續封鎖及保護。

二、內網資安政策自動化符規覆核平台：1 式

(一) 底層端點網路身分辨識管理系統

1. 具備 Web 管理介面，管理介面須包含英文及繁體中文語系。
2. 系統管理者帳號需支援不同驗證方式，至少包含本機帳號、AD 帳號及 Radius 帳號驗證方式，可支援 500 個(含)以上管理者使用管理。
3. 具備依登入使用者不同可進行分層授權，登入連線無授權數量限制，管理者帳號無使用上限，系統最高權限預設帳號可提交封存保管
4. 系統需由單一管理介面管理本案採購之硬體偵測器，未來並可擴充透過本現有網路設備之簡單網路管理通訊協定(SNMP)

來偵測 IP、MAC 資訊(集中式)之架構。

5. 系統可支援偵測器群組設定，可設定偵測器所隸屬的群組範圍，達到以下不同管理的需求，新設備接入時可單一 MAC 授權全單位放行或分不同群組個別授權。
6. 操作介面上須依本單位需求加入所需各項欄位，可新增、刪除欄位及調整欄位順序，方便管理者進行管理，並可依據欄位來做排序，欄位建立時需可支援 IP Base 或 MAC Base 兩種參照模式。(IP Base 意旨欄位資訊固定於 IP 資訊上，不會應設備異動而變更；MAC Base 意旨欄位資訊固定於 MAC 資訊上，當設備變更 IP 時，欄位資訊會跟著異動至新的 IP。
7. 各個自訂欄位可分別設定讀寫權限給不同管理者，且此權限與 Web Console 管控權限獨立運作，例如管理者 A、B、C 均可設定 IP 封鎖、IP 放行，但 A 可編輯自訂欄位"單位"、"部門" ； B 只可編輯自訂欄位"部門"，C 只可編輯自訂欄位"單位"。
8. 系統須具備依登入使用者不同可進行管理介面功能鍵隱藏之功能，例如 B 管理者可以看到匯出 IP/MAC 清單功能鍵，A 管理者無法看到匯出 IP/MAC 清單功能鍵，隱藏鍵功能至少包含欄位順序、欄位顯示，匯出 Excel 及系統設定功能鍵等。
9. 提供儀表板功能，可於儀表板違反政策之相關事件統計，並可於儀表板執行封鎖設備授權，儀表板亦支援分層授權設定，可依據不同的管理者設定儀表板資訊的啟用及停用。
10. 支援裝置識別功能，無須安裝用戶端軟體即可自動識別設備作業系統資訊，至少包含 Window、Linux、UPS、Switch、Printer、IOS 及 Android，並支援可手動定義多種設備識別規則，可依據不同欄位設定規則判斷。
11. 管理介面須具備搜尋功能，可依不同欄位自訂多個條件搜尋，例如管理介面只要列出 Printer 的設備清單，並可儲存

搜尋條件。

12. 管理介面需支援即時事件顯示功能，並可依據不同事件自訂嚴重等級紅、黃、藍燈燈號，以方便管理者識別。

13. 管理介面可以自行切換為基於 IPv4 及 IPv6 共存管理介面或 IPv4 及 IPv6 分開管理介面兩種不同模式,於共存管理模式可於統一管理介面顯示全單位 IPv4 及 IPv6 資訊，並可直接按右鍵直接設定 IPv4 或 IPv6 之 IP 相關管理、MAC 相關、IP-MAC 相關等管理政策。

14. 支援主機事前註冊之功能，提供管理者可事前授權設備以及設定相關綁定政策，並可支援單次及批次註冊。

15. 支援網卡製造商自動授權功能，可設定特定廠牌設備自動放行。

16. 可針對單位內空的 IP 即未使用的 IP 做上鎖保護，確保 IP 實名化落實執行。

17. 須可在單一管理頁面支援即時 IP 狀態、IP 事件、政策設定等資訊查詢，以利管理者方便管理並可在任一設備上按右鍵直接設定 IP 相關管理、MAC 相關、IP-MAC 相關等管理政策。

18. 本系統需支援針對不同之 IP 及 MAC 位址設定其網路使用期限及週期，可訂定多種不同時段，設定方式至少包含一次性設定(1 月 1 日 00:00- 12 月 31 日 11:59) 或週期性的設定(週一到週五 08:30-17:30)。

19. 系統需支援先佔 IP 保護功能，特定 IP 上設定此功能後可支援先上線的設備進行保護不受 IP 衝突影響，當兩台設備角色互換時亦能保護合法者，當政策生效時能夠看到先佔 IP 保護政策事件紀錄。

20. 支援特權 IP 管理功能，可針對特定 IP 設定白名單政策，該設定成白名單的 IP 不會受到其他封鎖政策影響。

21. 支援自動發信功能，當遇違反策略時，可自動寄發警告信

給管理者。且此功能支援分層授權管理機制，可針對不同管理者自由選擇欲通知之違反策略。

22. 可將系統事件資訊與告警(例如:某 IP 一段時間內每天上下線時間紀錄、某 IP 一段時間內自訂欄位變更修改的紀錄,…等)以 CEF 格式自動傳送到本單位 SIEM Server。

23. 本案提供 3000U (含)以上授權數量。

24. Log 紀錄可供留存(含)1 年以上。

(二) AD 進階管理系統

1. 支援 Agentless 及一般使用者權限，並支援多個網域目錄(Windows Active Directory)，並可將 AD 使用者登入登出資訊寫入內網資安政策自動化符規覆核平台，並可勾選所需之 AD 欄位。具備端末設備登出入網域紀錄包含即時資訊及歷史紀錄，例如: 一般登入、遠端登入、何時登入、何時登出、用哪個帳號、用哪台電腦均可提供查核。可長期保留記錄快速產生稽核報表以及具備登入次數統計報表，提供時段登入次數確認有無異常登入次數。
2. 提供網域內電腦 SID 重複檢查功能，無須安裝用戶端軟體，可掌握網域內用戶端電腦是否有 SID 重複的狀況。
3. 提供網域內電腦分享資料夾檢查，無須安裝用戶端軟體可檢查網域內用戶端電腦是否有自行分享資料夾。

(三) 內網資安政策自動化符規覆核平台- 報表系統

1. 須提供獨立的報表平台，報表平台需提供 Web 管理介面，管理介面須支援英文及繁體中文語系。
2. 報表平台需支援多位管理者同時進入系統操作，並針對不同管理者可自訂期可檢視的報表進行分層授權設定。(可由產品型錄證明)
3. 支援事件記錄查詢並可匯出成 excel 檔案格式。

4. 報表產出可以依據不同的篩選條件(IP/MAC/時間範圍/自訂欄位等)產出階層式報表（包含明細、圓餅圖、長條圖等)。
5. 支援自訂欄位篩選報表功能，管理者可依據不同自訂欄位定義不同值，產生對應之報表。
6. 支援報表訂閱功能，報表可自訂排程並寄發給不同管理者。
7. 具備以下報表功能包含日報表、週報表、月報表、季報表、事件增減統計表、 日(月)統計趨勢報表、IP 衝突事件報表、IP 逾期報表、登入登出網域歷程報表、未加入網域設備報表、GPO 政策套用檢查報表、本機最高權限檢查報表、未關機報表等。

備註：

1. 本採購案所開立規格須於驗收時截取系統畫面佐證
2. 承上除規格後面註明可用產品型錄證明之規格,若無法於系統畫面截圖證明時，可用原廠證明文件或原廠型錄佐證
3. 本案所需管理軟體主機之交付規格可為虛擬化架構主機或實體主機擇一交付，如為實體主機至少需符合以下需求：
   (1) CPU：Dual core 2.8 GHz 以上
   (2) RAM：32 GB 以上
   (3) Hard Disk： 200 GB 以上
   (4) Network：1 個 1GigaByte interface
   (5) 作業系統 Windows Server 2008 R2 / 2012 R2 / 2016 中文版
   (6) 需安裝 IIS,.NET FRAMEWORK 3.5 SP1
   (7) Microsoft SQL Server 2008 R2 Express OR 正式版

貳、交付項目表

項目	交付文件	數量
1	E-soft Dr.IP IP 管理系統軟體授權	3000U
2	E-soft AD 進階管理系統軟體授權數	2000U
3	Tracker 1000 (Support 5000 個 IP;200 個 C-Class;200 個 SNMP(2 port)	1
4	Tracker 100 (Support 500 個 IP;10 個 C-Class;12 個 SNMP(1 port)	2