網路流量智慧型分流及資安行為管控系統採購規格

壹、 設備採購通則要求

1. 本案採購之各類設備均需符合標準 19 吋機架規範，適用於本會機房安裝環境。
2. 本案採購之所有軟硬體皆須提供原廠新品證明、原廠連帶保固證明、軟體合法授權證明、原廠三年保固證明，所提供之軟硬體不得為已停產及未來一年內計畫停止銷售之產品。所提供之文件完整列出品名及數量。
3. 本案採購之設備需為國內製造之產品或國內廠商自行進口之國外廠商製造產品，但不可為中國大陸製造之產品，需提供原廠證明文件。
4. 須提供該設備相關完整功能所有的License安裝於設備上並需提供原廠證明文件，證明為合法License授權。
5. 廠商需將系統架構圖規劃撰寫於系統建置計畫書審核。
6. 於本專案中所提供之軟、硬體設備須提供原廠及保證不含任何惡意程式、後門、木馬程式、病毒及蠕蟲等證明。
7. 本專案計畫規劃使用產品，須有在台製造或代理之廠商提供對後續產品功能支援、說明之義務。
8. 廠商產品所提供之平台工具及設備均需支援 IPv6 及 IPv4 雙協定。
9. 各工作區對應之系統或設備數量如下（投標商為達容錯能力，高度可用性、避免單點失誤之整體建置需求，設備可以增加，但不得低於此數量）

工作區	數量
網路流量智慧型分流機制系統	1
網路流量智慧型分流機制交換器	2
網路流量智慧型分流負載平衡器	2

網路資安行為管控系統	2
網路資安行為傳輸加密系統	2
網路資安行為流量加解密系統	1
網路資安日誌集中報表系統	1

貳、 網路流量智慧型分流機制系統及網路資安行為管控系統需求說明

1. 網路流量智慧型分流機制系統可由單台或多台不同功能之設備組合而成。
2. 網路流量智慧分流機制導出之流量可同時支持 in-line 與 out-of-band 資安設備（IPS、Webfilter 或防火牆等設備）
3. 透過網路流量智慧分流機制，可自行調配將導入流量分散至多個納管於智慧分流系統內的不同資安設備上進行處理。
4. 具偵測資安設備之功能是否正常，如遇資安設備異常不通之狀況，可自動 bypass 異常的資安設備或是將流量導往其他資安設備，以避免網路服務中斷。
5. 規劃之網路流量智慧分流機制，若為多項設備組合而成者，需提供單一管理機制為宜，以方便該機制之管理與運作。
6. 網路資安行為管控系統與網路資安行為傳輸加密系統須建立 site to site vpn，不能有連線中斷之情形。
7. 網路資安行為管控系統及網路資安行為流量加解密系統須為同一家廠商之防火牆。
8. 網路流量智慧型分流負載平衡器，因本會 GSN 線路 IP 只有一個，須以一個 IP 兩條線路進負載平衡器的情況下達到 HA 功能，禁止加裝其他設備。
9. 協助將舊有網路負載平衡器 A10 TH930 轉換成伺服器負載平衡器，並教育訓練。
10. 須於各設備主機外觀上標示清楚各設備名稱。
11. 系統連接的網路或光纖線路須清楚標示線號。
12. 驗收測試完成後須提供系統架構圖電子檔，架構圖上須清楚表示線號及設備名稱，電子檔須為可修改之檔案。
13. 需將舊有設備之相關設定傳換到新設備上。
14. 更改對外網路系統架構，需將現有防火牆上的網路位址轉換功能轉

換到新購的網路流量智慧型分流負載平衡器上。

15. 智慧分流機制，須整合本會既有之資安設備與骨幹網路設備，並符合以下功能：

（1） 每一攝影棚之對外使用頻寬可依時間進行最大頻寬使用量之限流。

（2） 通往 DMZ 區的流量需經過指定設備進行資安防護。

（3） 一般使用者流量可流經指定設備進行資安防護。

（4） 特定之流量，需先流經 SSL 解密設備進行內容解密，再流經指定資安設備清洗，最後回到 SSL 加密設備進行內容加密，再將流量送往 Intertnet 或使用者。

（5） 以上所描述的指定設備僅包含此案新購入之資安設備及現有的 WAF(F5)

參、 網路流量智慧型分流機制系統設備規格

一、 網路流量智慧型分流負載平衡器(共 2 台)

1. 獨立主機採硬體式設備(Hardware Appliance)架構，設備需採用非 Windows/Unix 系列的高安全性之嵌入式即時作業系統(Embedded Real-Time OS)。且須提供 6 埠(含)以上 10/100/1000 TX 網路介面， 2 埠(含)以上 1Gb Fiber 光纖介面(SFP)。
2. Concurrent sessions 須達 2,000,000(含) 以上及整體處理效能 Throughput 須達 2Gbps(含) 以上，日後可原機擴充將 Throughput 擴充至 4Gbps(含) 以上。
3. 本設備對外線路數須支援 100 筆以上
4. 須提供站點名稱(Host Name)解析 IP 之需求。
5. 須支援網路位址轉換功能(NAT)，其中包含靜態通訊埠 NAT、動態多對一 NAT、靜態一對一 NAT，並至少提供 8,000 個 NAT IP 位址之需求。
6. 提供 Router 或 Bridge 功能，支援靜態路由與動態路由 RIP v1/v2、OSPF、VRRP 雙機備援。
7. 本設備須支援不同 ISP 線路之上傳(Inbound)及下載(Outbound)多線路負載分配管理功能。
8. 本設備須同時支援防火牆及 VPN 負載平衡。並提供點對點 VPN 連線

在多個 ISP NAT 線路間切換不需重建連線之需求。

9. 本設備可以針對客戶需求，依照 Source IP、Destination IP、TCP/UDP 應用埠 Service Port，及 HTTP 內容來指定特定線路，並針對線路群組套用不同的負載平衡及備援政策。
10. 具備內建第七層負載平衡功能，無需編輯任何 TCL 或 Script 語法即可依照 HTTP URL、path、file name、file type、header、cookie、DNS Query 進行分配。
11. 本設備須提供下列負載分配模式:
    (1)循環模式(Cyclic)。
    (2)依線路最少流量者優先分配模式(Least Traffic)。
    (3)依線路最少使用者優先分配模式(Least User)。
    (4)依線路最快回應時間優先分配(Response Time)。
    (5)依線路之權重分配(Weight)。
    (6)依線路之使用成本分配(Cost)。
12. 本設備須可提供動態與靜態就近性功能(Proximity)，能有效的對網站和資料中心所託管的外聯網應用的訪問時間減至最少，亦可將內部用戶對關鍵外部網路資源的訪問時間減至最少。
13. 提供限定各線路同時可提供服務之最大連線數、限定上傳及下載之最大可使用頻寬數、服務回復後之漸進式負載指派等過載保護機制，須可設定 ”線路恢復時不指派流量之時間秒數” 及 ”漸進式負載指派之時間秒數”。
14. 當線路出現異常或達到過載保護量時, 須以 Email, Trap 及 SYSlog 通知管理者。
15. 使用者已建立之連線須保持其在原線路上使用，直到連線關閉。對於閒置於各線路之連線可依應用類別訂定其最高之可閒置時間(Aging time)。
16. 提供 ARP、Citrix App Browsing、Citrix ICA、DHCP Discovery、PING、TCP/UDP Port、HTTP Content、SMTP Hello、IMAP4 Login、POP3 Login、RADIUS Login、RTSP、SNMP、DNS Query、FTP Login、SSL Content、LDAP 等方式，自動判斷各個指定之檢測點可用性。
17. 上述之各個檢測點可依需要訂定為”必要檢測點”及”非必要檢測點”，並指定為同一判斷群組。當任一”必要檢測點”無法回應，或是當所有之”非必要檢測點”均無法回應時，此一相關之判斷群組即宣告健康檢測錯誤，其相關之網路或伺服器資源不再參與負載分配任務，直到其健康檢測無誤。
18. 內建防禦 DOS 攻擊功能，可以針對 SYN Flood 入侵防禦行為進行阻絕。
19. 須提供與紀錄使用者歷史和即時路由分派資訊列表，並可以透過匯

出的方式供管理人員後續查詢與稽核之用，內容資訊需包含:
(1)開始使用時間。
(2)結束使用時間。
(3)來源 IP 及 來源應用埠(Source Port)。
(4)目的 IP 及 目地應用埠(Destination Port)。
(5)使用之線路。
(6)使用 NAT 的方式。
(7)NAT 以後的 IP 位址。

20. 網管設備與所有設備間須提供加密方式連線管理,須可限制管理者由特定之任意實體介面進入控管。
21. 本設備須支援下列管理介面方式與通訊協定：
(1)HTTP。
(2)HTTPS。
(3)TELNET。
(4)SSH。
(5)SNMP。
(6)Console。
22. 本設備須支援中央管理設備平台進行統一管理,達到三層式管理架構，提升設備的安全性。
23. 符合標準 19 吋機架式規格或可安裝於 19 吋機櫃。

頻寬管理功能:(Optional)

24. 本設備須可擴充以下頻寬管理功能：
(1)依據下列條件設立策略：
A. 來源 IP。
B. 目的 IP。
C. 應用埠 (Port)。
D. 實體端口。
E. 啟用與停止時間。
(2)每一策略可獨立設定下列功能:
A. 保障頻寬, 頻寬設定以 1Kbps 為基本單位。
B. 可使用之最大頻寬, 頻寬設定以 1Kbps 為基本單位。
C. 每一來源 IP 可使用之最大頻寬, 頻寬設定以 1Kbps 為基本單位。
D. 每一來源 IP 同一時間可使用之最大連線數。
E. 每一來源 IP 對同一目地 IP 可使用之最大頻寬, 頻寬設定以 1Kbps 為基本單位。
F. 每一來源 IP 對同一目地 IP 同一時間可使用之最大連線數。

(3)針對個別策略提供即時與歷史圖形流量報表。
(4)提供前五大最主要流量使用策略報表。

25. 提供限制不特定之單一個別 Client 同時可使用之連線數目，提供避免資源獨佔之需求。

二、 網路流量分流機制交換器(共 2 台)

1. 介接之資安設備，可指定不同的規則，並可依不同設備順序，訂定不同之連續規則。規則條件至少具 MAC Source 或 Destination address、IP Source 或 Destination address、IP Subnets、Ethertypes、VLAN ID、TCP/UDP port number，其中 IP address 須同時支援 IPv4 與 IPv6。
2. 須支援 OpenFlow Switch Specification v1.3.0 版本(含)以上。
3. 單一台開放流交換機之系統總 Flow Entries 數量須支援 16,000 筆(含)以上。
4. 須支援 L4 (含)以下欄位，同時 Match 且 Wildcard Match 的 Flow Entries 數量須支援 4K 筆, Exact Match 的 Flow Entries 數量須支援 1M 筆(含)以上。
5. Flow Entries 須支援 OpenFlow Switch Specification v1.3.0 版本(含)以上的
6. Match Field，包含 Ingress Port、Ethernet Source/Destination Address、 Ethertype、IEEE 802.1Q VLAN ID、IEEE 802.1Q VLAN PCP、 ICMPv4_TYPE、ICMPv4_CODE、IPv4 Source/Destination Address 、 IPv4 Protocol 、 IPv4 DSCP Bits 、 IPv6 Source/Destination Address、TCP Source/ Destination Port、UDP Source/Destination Port。
7. Flow Entries 須支援 OpenFlow Switch Specification v1.3.0 版本(含)以上的 Action，包含 Output、Forward Flood、Drop、Set-Queue、Push(VLAN Tag) 、 POP(VLAN Tag)。
8. Flow Entries 須支援 OpenFlow Switch Specification v1.3.0 版本(含)以上的 Set-Field Action，Set-Field 欄位包含 Ethernet Source/Destination Address、 IEEE 802.1Q VLAN ID、IEEE 802.1Q VLAN PCP、IPv4 Source/Destination Address。
9. Flow Entries 須支援 Idle 與 Hard timeout。
10. 支援 Per-flow 的 Meters 與 counter，整台系統總數量均須個別支援 8000 筆(含)以上。
11. 支援 Group Table 須包括 Group Type: Indirect, All, Select, Fast Failover。
12. 整台系統支援 4 張(含)以上 flow table

13. 系統總 Throughput 須達到 140 Gbps（含)以上。
14. 須提供 16 埠(含)以上 10Gigabit Ethernet 介面(含 16 個含以上 10G-SFPP-SR)
15. 開放流交換機之任意兩個網路埠間延遲不得高於 1ms。

肆、 網路資安行為管控系統設備規格

一、 網路資安行為管控系統(共 2 台)

1. 獨立主機採硬體式設備(Hardware Appliance) 架構，並使用嵌入式或專屬作業系統(無硬碟),本身提供 18 埠(含)以上 10/100/1000 Mbps(含)以上速率連接埠介面 ，提供 4 埠 Fiber 介面 (SPF)。
2. Concurrent sessions 須達 2,000,000 個(含) 以上及整體處理效能 Throughput 須達 20Gbps(含) 以上，IPsec VPN Throughput 須達 9 Gbps(含)以上， New Session 可達 135,000(含) 以上
3. 提供網路低延遲時間,效能至少達 3 us
4. 具備網路位址轉譯(NAT(Network Address Translation))及埠位址轉譯(PAT(Port Address Translation)) 功能
5. 具備 IPSec VPN 或 SSL VPN 功能，加密演算法支援 3DES(Data Encryption Standard)及 AES(Advanced Encryption Standard)，且 3DES 處理效能 Throughput 須達 9Gbps (含)以上，並提供 IPSec 或 SSL VPN 資料傳輸內容檢查(inspection)
6. 具備 URL Block 及 Java Applet 、ActiveX 過濾的功能
7. 提供無線基地台控管功能，無需增購授權。至少可控管 128 顆 AP
8. 支援網路防毒功能，有效阻擋網路病毒、蠕蟲的侵害，並可選購病毒碼自動更新服務，NGFW Performance 可達 1.8Gbps (含)以上
9. 提供入侵偵測功能，Performance 可達 6Gbps (含)以上，可偵測 backdoor、port-scan、Web-based 攻擊以及利用 SQL 作為跳板的攻擊 可阻擋 TCP SYNflood、port scan、ICMP flood、ICMP land、IP spoofing、ICMP Death、UDP over limit session、FTP SMTP overflow 等等。
10. 具備 URL Block 及 Java Applet、ActiveX 過濾的功能及具體網頁分類功能，保護使用者網頁瀏覽之安全。
11. 具記錄管理(Syslog/Event logs) 和警訊(alarm)，另可透過本機或經由中央管理軟體提供 E-mail notify 功能
12. 具備網頁式或 Java 管理設定介面
13. 具備韌體更新系統及組態異動功能
14. 提供虛擬防火牆功能，至少可設定 10 組之虛擬防火牆，以提供不同之防火牆政策佈署。.

15. 通過 ICSA Antivirus 認證 及 ICSA IPSec 認證 及 SSL VPN 認證及 ICSA Firewall 認證, ICSA IPS 認證。
16. 符合標準 19 吋機架式規格或可安裝於 19 吋機櫃
17. 具備應用程式識別功能
18. 提供殭屍網路(Botnet 或 Zombie)偵測與阻擋功能，防止因內部用戶感染了惡意(Malware)軟體或間諜(Spyware)軟體進行殭屍病毒通訊，即防止分散式阻斷服務攻擊(Distributed Denial of Service)程式,將淪陷的機器即僵屍電腦,組織成一個個控制節點,用來發送偽造包或者是垃圾資料包,使預定攻擊標的癱瘓並「拒絕服務」
19. 提供 IPv4 和 IPv6 防火牆防護、IPS 入侵防禦、AntiVirus 網路病毒過濾、阻斷 DoS 攻擊，以及主動隔離異常來源 IP 等多項資安防護功能。
20. 通過 IPv6 Phase2 Ready 安全認證。
21. 廠商技術須通過 FIPS 140-2 和 Common Criteria EAL 4 (ISO/IEC 15408) 安全等級認證。
22. 支援網路設備 HA(High Availability)或 Failover 備援功能，使單機發生故障無法運作時，備援設備(請訂購機關依各別需求另行增購)可接續運作。
23. 具備 Web-based 管理介面。
24. 操作管理介面與報表系統須支援英文、中文等多國語系。
25. 提供詳細的用戶身份定義對應(Identity-based policy)規則,可依據不同參數將使用者對應至不同角色及不同權限。
26. 用戶端設備種類辨識功能 (Android, Apple, BlackBerry, IP Phone, Mac, Windows, Linux, Fortinet , Gaming Console)
27. 提供應用程式管控功能,可以針對不同的使用者定義所屬的應用程式及 QoS 政策。
28. 支援 LDAP 或 RADIUS 或 Active Directory 使用者認證。
29. 操作管理介面與報表系統須支援英文、中文等多國語系。

二、 網路資安行為傳輸加密系統(台中中部新聞中心 1 台，高雄南部新聞中心一台，共 2 台)

1. 獨立主機採硬體式設備(Hardware Appliance)架構，並採用 SPU (ASIC) 晶片模組設計。並使用嵌入式或專屬作業系統，本身提供 10 埠(含)以上 10/100/1000Mbps(含)以上速率連接埠介面。同時具備 1 埠專屬管理介面。。
2. 系統最大連線數須達 1.3 Million 個(含)以上，以及新增連線數須

達 30,000 個(含)以上。

3. 廠商需提供佐證文件或測試數據，防火牆處理效能 Throughput 須達 3 Gbps(含)以上，IPsec VPN Throughput 須達 2 Gbps(含)以上，且封包 64bytes 網路延遲時間不得高於 3 微秒(μs)。
4. 廠商需提供佐證文件或測試數據，當 NGFW 等功能全部開啟的狀態下處理效能 Throughput 須達 250 Mbps(含)以上。
5. 廠商需提供佐證文件或測試數據，當入侵防護、應用程式管控、防毒系統和惡意程式阻絕等功能全部開啟的狀態下處理效能 Throughput 須達 200 Mbps(含)以上。
6. 廠商需提供佐證文件或測試數據，當入侵防護功能開啟的狀態下處理效能 Throughput 須達 1.4 Gbps(含)以上。
7. 廠商需提供佐證文件或測試數據，當應用程式管控等功能開啟的狀態下處理效能 Throughput 須達 650 Mbps(含)以上。
8. 提供最高達 5,000 個(含)以上的安全策略(Security Policy)。
9. 具備網路位址轉譯(Network Address Translation, NAT)、埠位址轉譯(Port Address Translation, PAT)功能及具備 Carrier-grade NAT 或同等電信等級轉址技術。
10. 具備以國家別或地域名稱來制定流量過濾、阻擋政策功能(Location / GeoIP / Geography)，及時預防可能隱藏的駭客攻擊威脅，須可主動過濾大量或大範圍的異常國際網路連線(例如北韓、菲律賓)。
11. 具備 10 個(含)以上虛擬防火牆功能。
12. 具備三種檢測模式：路由模式、透通模式、旁聽模式(Sniffer 或 Span)
13. 資安政策可依照每週、每日及特定時間排程來設定生效期間，並能顯示設備開機後，防火牆政策符合連線數的總計，並在同一頁面顯示此政策最後連線時間、首次連線時間。
14. 具備同時支援多種使用者資料庫（Radius、LDAP、TACACS+、Local DB、POP3）之使用者驗證，以利符合多元網路使用者環境之佈署與控管。
15. 具備記錄管理 (Syslog/Event logs)，另可透過本機或是經由中央管控系統，提供電子郵件通知功能。
16. 具備正體中文圖型化管理介面，需提供即時網路資訊觀看功能。
17. 通過 IPv6 組織驗證測試，具備 IPv6 Ready Logo Phase2 認證文件。
18. 具備威脅世界地圖功能於網頁介面，可即時觀看世界地圖得知威脅來自於地圖上的國家。(僅支援內建儲存設備)
19. 支援透過 Internet Service Database 做為防火牆政策的目的物

件，包含 Adobe、Amazon、AOL、Apple、Cisco、Google、Microsoft、Yahoo…等等通用服務供應商網站 IP。

20. 廠商技術須通過 ICSA Firewall、NSS Firewall 等國際第三方實測安全認證，廠商須提供至今仍然有效的證明文件。

三、 網路資安行為 SSL 流量加解密系統(共 1 台)

1. 獨立主機採硬體式設備(Hardware Appliance)架構，並使用嵌入式或專屬作業系統，且須提供 6 埠(含)以上 10/100/1000 TX 網路介面， 2 埠(含)以上 1Gb Fiber 光纖介面(SFP)與 4 埠(含)以上 10Gb Fiber 光纖介面(SFP+)。
2. 內建 16G 記憶體，並使用 SSD 固態硬碟。

   具備下列 SSL 流量處理效能：

   (1) SSL 加解密服務處理效能至少需達 2.5 Gbps (含)以上。

   (2) SSL RSA 處理效能至少需達 12K CPS(Connections Per Second)(含)以上。

   (3) SSL ECDHE-ECDSA 或 ESCSA-P256 處理效能至少需達 7 K CPS(Connections Per Second)(含)以上。

   (4) SSLi Concurrent Sessions 至少需達 200K
3. 支援 ICAP 通訊協定，將 SSL 拆解流量傳遞至支援 ICAP 協定至防毒閘道及資料外洩解防禦系統(DLP)等資安系統檢查。
4. 具備以下 SSL 流量處理能力：

   (1) TLS 1.0/1.1/1.2 及 SSLv3。

   (2)RSA、DHE、ECDHE，符合 Perfect Forward Secrecy (PFS)。

   (3) SHA、SHA-2、MD5 雜湊演算(hashing algorithms)。
5. 支援以下 SSL 加解密演算法：

   (1)TLS_ECDHE_ECDSA_WITH_AES_128_ CBC_SHA

   (2)TLS_ECDHE_ECDSA_WITH_AES_256_ CBC_SHA

   (3)TLS_ECDHE_ECDSA_WITH_AES_128_ CBC_SHA256

   (4)TLS_ECDHE_ECDSA_WITH_AES_128_ GCM_SHA256

   (5)TLS_ECDHE_ECDSA_WITH_AES_256_ GCM_SHA384
6. 提供以下 SSL 條件式排除，不做加解密動作服務：

   (1)依據網站名稱

   (2)依據 IP 地址
7. 具備硬體 SSL(Secure Sockets Layer)代理(Proxy)與卸載(Offload)功能，並支援 4096-bit(含)以下金鑰加解密功能。
8. 具備 SSL 加密流量拆解能力，將 SSL 上網流量拆解為未加密流量後交由資安設備檢測，資安設備檢測完流量需重新封裝為 SSL 流量，以不妨礙正常上網流量。

9. 系統需具備 Bash，Python 及 Perl 等嵌入程式之健康檢查方法，針對伺服器進行多層步驟、複雜的健康檢查。
10. 提供 Web Application Firewall 功能，並通過 ICSA Labs WAF 認證。
11. 系統需具備 TCL 腳本編程功能，可使系統管理員依據應用內容之資料做為負載均衡之依據。
12. 提供 CLI(Command Line Interface)、SSH 命令列管理介面與 Web GUI 管理介面，並可提供事件紀錄及韌體更新等功能 。
13. 提供應用程式開發介面（API)，以利第三方客制化應用程式整合。
14. 符合標準 19 吋機架式規格。

四、 網路資安日誌集中報表系統(共 1 台)

1. 單一機體,可提供安全閘與日誌主機間通訊資料加密轉輸.
2. 具 2 埠 Fast Ethernet 10/100/1000Mbps 自動偵測
3. 內建 4TB 硬碟
4. 支援英文、中文等多國語系管理介面。
5. 高達 4500 日誌/秒，可管理 150 台設備，每天最高接收 100GB logs
6. 內建 LOG 儲存功能，並可依時間、來源位址、目標位址等設定搜尋條件，並能以關鍵字搜尋過濾其日誌資料，並能將 log 輸出至統計報表。
7. 能紀錄 Email 收/送信者,主旨,內容，所瀏覽的 URL 明細，且 log 可輸出至統計報表工具。
8. 支援 PDF 格式的報表輸出。
9. 提供及時的警告訊號，可透過 E-mail 告知，以做即時之處置。
10. 可提供設備全範圍的日誌記錄，包括流量、時間、病毒、攻擊、內容過濾和郵件過濾數據。
11. 可新增管理使用者，設定分權管理。
12. 系統管理提供 Console / Web UI，支援遠端管理，可使用 IE 瀏覽器遠端登入設定查詢報表資料
13. 支援其他 syslog 兼容設備上收集到的各種數據，對其進行安全的聚合，分析和報告。

（一）、 教育訓練(免費)

系統安裝完成後，即可進行全單位教育訓練，並於裝機完成日起 60 個日曆天內完成。立約商準備教育訓練計畫，並提供原廠或原廠教育訓練合格

證教師在指定之時間及地點進行教育訓練課程，單項課程至少 16 小時以上之專業訓練，並得視使用單位需要延長，惟單項課程總天數以 30 天為限，立約商並不得另外要求收費。師資人員及其他相關衍生性之所有費用皆由立約商自行負擔，教育訓練課程內容，必須包括系統操作與維護。不限上課時間、梯次。

立約商至少須對公視基金會人員，提供以下項目之教育訓練課程服務：

1. 網路流量智慧型分流機制系統教育訓練(至少 2 次)
2. 網路流量智慧型分流負載平衡器教育訓練（至少 2 次）
3. 網路資安行為管控系統教育訓練（至少 2 次）
4. 網路資安行為傳輸加密系統教育訓練（至少 2 次）
5. 網路資安行為流量加解密系統教育訓練（至少 2 次）
6. 網路資安日誌集中報表系統教育訓練（至少 2 次）
7. A10 TH930 伺服器負載平衡器教育訓練（至少 2 次）

配合上述之需求，立約商須提供完整之使用者及管理者教育訓練計畫。

立約商須提供規劃之教育訓練時程、課程內容、授課師資、課程進行型態、課程實施地點、課程技術等級、教育訓練時數、人數等。

系統上線後四個月內，公視基金會安排適當種子人員，至多不超過十位，立約商需提供原廠教育訓練。種子訓練課程內容需先提給公視基金會審核，認可後才能執行。

驗收前，立約商應製作全系統中文操作手冊，作為驗收項目之一。

保固期間之教育訓練內容，應編寫入保固維護計畫書內。

（二）、 其它

交貨

1. 需於簽約後 60 個日曆天內完成交貨。每遲延一日，應分別按各批契約價款千分之一逐日計課逾期違約金，上限為契約總價百分之二十。

系統建置

1. 立約商應於簽約日起 30 個日曆天內繳交工作計畫書初版，通過公視基金會認可。內含各階段工作項目、交付項目、時程等系統建置導入計畫，作為本系統開發時程進度管控依據。
2. 立約商應進行系統需求分析與使用者訪談，提出「系統建置計畫書」，並於完成交貨日前，通過公視基金會認可，並作為驗收之依據。
3. 立約商應於簽約日起 60 個日曆天內完成交貨。
4. 立約商應於交貨日起 30 個日曆天內完成裝機，裝機完成後需提報本會裝機完成日期，以訂為合約裝機完成起始日。
5. 立約商於裝機完成日起 30 個日曆天內，提供測試驗收計畫書，並經公

視基金會核可，據以辦理測試事宜，內含測試之項目、格式、測試方法、品質參考值供測試。

6. 立約商應於裝機完成日起 60 個日曆天內開始啟動系統測試，該日期訂為合約系統測試起始日。

7. 系統測試日起開始 60 個日曆天內，立約商必須通過各項實機測試，否則無法提報驗收，並開始計罰，每日計課總契約金之千分之二罰款。

裝

訂

線

驗收測試

本採購案相關軟硬體設備之整體運作測試，於裝機完成日起 30 個日曆天內提交並經由公視基金會核可之測試驗收計畫書（內容應延續專案建置計畫書範籌），進行各項測試，測試通過後始得手日人報辦理驗收。測試開始為期 60 日曆天內完成，（需通過多次驗證）未能如期完整測試通過，即開始計課罰款，每遲延一日按契約總價款，千分之二逐日計課罰款。

立約商所提之測試計畫，應進行逐項測試驗證，並通過實地隨機抽驗，測試至少需包含以下測試項目：

（一）壓力測試：24 小時連續 30 天網路及監測系統正常運行，必須有網路流量。

（二）復原測試（壓力測試時同步執行）：驗證整體系統是否具備完整的安全性備援設計（無單點失效造成系統無法進行運作），並觀察備援機制的可靠性。

以上測試，不能有斷線或影響內部系統之狀況發生。測試期間發生問題需要修正，條正後必須重測壓力測試及復原測試，修正及重測之日期為測試開始為期 30 日曆天內完成（包含重測壓力測試及復原測試）。

測試過程之品質標準、驗證次數，應明訂於測試驗收計畫書中並經公視基金會核可。

系統轉移時間須配合本會離峰時段:

項目	時間	執行要點	備註
1	22:00~24:00	1. 舊系統轉移至新系統。	轉移成功-執行項目 2 第 1 點。 轉移失敗-執行項目 2 第 2 點。
2	24:00~02:00	1. 新系統轉移後測試功能。 2. 舊系統復原。	
3	02:00~03:00	1. 舊系統復原後測試功能。	

保固與維護

1. 廠商應於測試通過日起 30 個日曆天內，提供「保固維護計畫書」，並經由公視基金會核可。計劃內容須提供完整保固計畫，以附註條款及本招標規範中保固項目相關條文為主要內容。
2. 本案自驗收合格日之次日起，立約商提供軟硬體三年 7*24 保固與維護，叫修後 4 小時內到府服務，如無法於 24 小時內修復完畢，立約商須無條件提供相容同等級以上之備品。
3. 若立約商無法在上述時限排除故障時，又無替代故障設備之措施時，則每逾期一日按該項設備契約價款之千分之二連續罰款至故障完全排除為止。罰款自保固保證金內扣收。
4. 保固期間內系統有任何異常，包含硬體損壞與軟體不正常運作，立約

商需提供免費維修及更換料件服務。

5. 於保固期內，提供每季一次到府設備檢修服務、備份設定檔。

6. 於保固期內，若因公視基金會業務需要，需進行設備關機、移機等工作，立約商需無條件派員技術配合處理，因異動產生之材料費用，由本會負擔。

7. 除特別註明不同保固時間之項目外，立約商需在保固期間內提供免費負責標的物之維修、保養換件等之維護工作，及在正常操作情況下發生故障免費修理與更換零組件。若標的物在保固期間內軟硬體有缺點(BUG)，立約商應負責維修或更新改善，並不得索取任何費用。

8. 立約商須於交貨時提供所有軟硬體設備三年之保固切結書及原廠連帶保固證明書。該切結書及證明書必須隨附購案中各項電腦系統軟硬體之個別廠商證明文件作為附件。

9. 全系統操作手冊不定期更新。

合約解除或終止

有下列情事之一者，本會得隨時解除或終止合約，其因此所受之一切損失，得標廠商應付賠償之責：

1. 因可歸責於得標廠商之事由延遲合約進度，顯可預見其不能於期限內完成者。

2. 合約進行中，得標廠商有違反本合約之情事，經本會告知後，仍不依

限期改善或依合約履行者。

規格審查合格標準

1. 書面審查，投標廠商須製作規格審查表(格式如附件一)，依各項設備所列之規格逐條答覆，並檢附相關佐證資料(產品型錄、技術手冊及原廠之相關技術文件)，須劃線並標示對應之規格項目編號，以利公視基金會審查。

裝

訂

線

附件一 規格審查表

▪ **規格審查表**

公共電視XXXXX案設備規範審查表

	規　　格　　說　　明	投標設備品名/型號	佐證文件頁次	佐證項目編號	應答說明	審核結果(廠商勿填)

註：1.將符合本規範之硬體設備型錄(正本或影本，影本應註明與正本相符，並加蓋公司章及負責人章)以螢光筆將符合本規範需求部份標示出來，並依本規範審查表之規定標示。

2.各項型錄、技術手冊皆須蓋投標廠商之公司章及負責人印章。

裝　　訂　　線