109年資安及外部網路管控系統採購規格

壹、 專案說明

一、 專案目標

1. 為達到資通安全責任等級A級之特定非公務機關應辦事項，透過本案應完成網路防火牆、入侵偵測及防禦機制、應用程式防火牆及進階持續性威脅攻擊防禦措施、SSL 加解密功能、網頁過濾功能及網頁應用程式防火牆之資通安全防護。
2. 於本案建置時更改網路位址轉換架構，由兩層更改為一層，需將防火牆上的所有網路位址轉換轉移至負載平衡器處理，並透過更改後的架構調整相關設定。
3. 透過 防火牆集中化管理平台系統(防火牆中控及報表分析)達到持續性資安防護分析監控功能、北中南防火牆集中管理功能及資安報表管理功能。

二、 廠商資格

1. 為確保資訊安全及得標廠商所提供的服務水準，得標廠商應符合下列條件，並於服務建議書專章詳述：

(一)凡在政府機關登記合格，無不良紀錄之廠商(檢附設立及登記證明、納稅證明及信用證明) 且不得為陸資企業(包括子公司、分公司、獨資或合夥事業及其轉投資事業)。本案服務人員需具有中華民國國籍，不得為外籍勞工或大陸來台人士。

(二)本案服務內容將涉及敏感資訊，得標廠商不得轉包或分包予其他廠商執行。

(三)投標廠商須實施資訊安全管理制度，通過 ISO 27001:2013，並於專案執行期間持續有效，以保護資安健診所取得之資料。

(四)本案團隊人力至少應包含專案負責人/專案經理與資安服務人員。資安服務人員應具備以下所列舉之技能，且各類技能至少有一名成員，以確保服務水準，並檢附成員姓名、訓練證書或專業證照等影本以供審核。應具備必要資訊網路、系統技能說明如下:

1.網路管理：接受過 CCNA (Cisco Certified Network Associate)。

2.資安系統：接受過 CISSP (Certified Information Systems Security Professional)。

3.技術人員證照：本案廠商所提供的設備，技術人員需有該廠牌之技術證照，以證明技術人員具有建置能力。

(五)廠商需提供原廠經銷授權證明，證明其為合法銷售廠商。

三、 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（不得為中國大陸製）。
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. 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。
7. 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。
8. 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）

產品	數量
線路及廣域式負載平衡器	2(B棟)
防火牆暨SSL加解密系統 (SSL加解密功能可用另外設備達成)	4(B棟2台，中、南部各1台)
GSN防火牆	1（B棟）
10G網路交換器	2（B棟）
L2 1G網路交換器(24Port)	2（中、南部各1台）

防火牆集中化管理平台系統	1 式(防火牆中控及報表分析)
網頁應用程式防火牆	1 (B 棟)

貳、 軟、硬體採購規格

一、 線路及廣域式負載平衡器需求規格(共 2 台)

(1) B 棟線路及廣域式負載平衡器(共 2 台)

1. 須具備 4 個 1000BASE-T Ports SFP 連接埠及 2 個 10 Gigabit Fiber Ports SFP+ SLOT 連接埠。
2. 至少須提供 2 個(含)以上電源供應模組，電源供應模組具備備援(Redundant)及熱抽換(Hot-Plug or Hot-Swap)功能。
3. 本設備具備 16GB RAM (含)以上。
4. 資料處理能力：
   A) L4 每秒連線處理能力(Connections Per Second)須可達 125,000 connections (含)/秒以上。
   B) L7 每秒需求處理能力(Requests Per Second)須可達 350,000 request(含)/秒以上。
   C) L4/L7 流量處理能力可達 10 Gbps(含)以上。
   D) 最大連接數可達 14,000,000。
5. 具備 3Gbps 壓縮能力，能對網頁內容進行壓縮。
6. 可依服務成長需求，添購授權以擴充原機連線處理能力，無須額外加購設備。
7. 本設備須提供 10 個使用者同時上線透過 SSL VPN 連線。
8. 支援 Layer 7 的內容操控 (包含插入/移除/修改第 7 層的內容)
9. 本設備須具備以下多種負載平衡模式：
   A) Round Robin(輪流)
   B) Ratio(權重)
   C) Least Connections(最少連結)
   D) Fastest(最快回應時間)
   E) Priority(優先順序)。
10. 本設備須支援連線堅持(Persistence)技術

    A) Cookie persistence

    B) Destination address affinity persistence

C) Hash persistence

D) Microsoft Remote Desktop Protocol persistence

E) SIP persistence

F) Source address affinity persistence

G) SSL persistence

11. 具備 Global Server Load Balancing(GSLB)廣域負載平衡及內建 DNS 功能，並能回應 A，CNAME，MX，SRV，AAAA。
12. 本設備須具備下列健康狀態檢查功能：
    A) Layer 3 checking：ping(ICMP)
    B) Layer 4 checking：port service
    C) Layer 7 checking：延伸內容檢查(Extended Content Verification)
    D) Application Level：HTTP/NNTP/FTP/SMTP/POP3/IMAP/RADIUS 及使用者自訂 script。
13. 具備專線負載平衡(Link Load Balancing)功能，支援以 Layer2 透通方式，Layer3 方式、NAT 等方式進行混合負載平衡
14. 可自動偵測 DDoS(Distributed Denial of Service)攻擊行為並產生阻擋，以保護後端伺服器不會因為遭受攻擊而導致服務中斷。
15. 本設備支援三台(含)以上之備援模式，至少提供一種（含）以上備援連線方式，包括：Network Failover..等
16. 本設備須可支援 IPV6 gateway 功能
17. 本設備須具備以下位址轉換功能：NAT、SNAT(Source NAT) 。
18. 支援 HTTP 1.0 與支援 HTTP 1.1 之間可進行轉換。
19. 可過濾 HTTP Session 中的特定字串，並直接拒絕中斷連線。
20. 具備 Route Domain，提供不同 Routing table，提供多元路由轉送。
21. 需內建 DNS 服務，提供標準 DNS SOA, A, AAAA, CNAME, MX record，並可支援 DNSSec 安全服務
22. 提供 DNSSEC 功能，提供設定 Zone Signing Key 及 Key Signing Key 自動產生功能，提供網路安全性用戶端與服務端公私鑰比對。
23. 自動控制全區 DNS 記錄更新檔案無需重啟 DNS 服務。
24. DNS 演算機制除了主要演算法之外還支援次要演算法及備援演算法。
25. 至少具備下列廣域網路負載平衡演算法：

    A) Round Robin

    B) Ratio

C) Global Availability

D) Topology

26. 整合伺服器或後端負載平衡系統狀態及上述監控條件做複合負載平衡
27. 可支援針對每個 Domain name 做 DNS TTL 客制化。
28. 提昇本單位 DNS 服務整體效能，需將本單位外部 DNS 服務轉移至本案採購之設備並支援 DNS 通訊協定 AXFR、IXFR，提供 DNS 服務卸載功能。
29. 可提供 DNS BIND 功能。
30. 內建 DNS 解析紀錄視覺化統計資料，可分析 DNS 查詢的資料。

裝

二、 防火牆暨 SSL 加解密系統規格

（1） B 棟防火牆及 SSL 加解密系統(共 2 台)

訂

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，本身提供 8 埠(含)以上 GE RJ45 介面和 4 埠(含)以上 10Gbps SFP+介面。同時具備 1 埠專屬管理介面，和 1 埠專屬 HA 介面。
2. 至少須提供 2 個(含)以上電源供應模組，具備備援(Redundant)電源供應模組。
3. 系統最大連線數須達 800 萬個(含)以上，以及新增連線數須達 67,000 個(含)以上。
4. 廠商需提供佐證文件或測試數據，應用程式可辨識 7,000 種(含以上)並當應用程式管控功能開啟的狀態下處理效能 Throughput 須達 3.7 Gbps(含)以上。

線

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 1.8 Gbps(含)以上。
6. 具備 IPSec VPN 連線方式，加密演算法至少支援 3DES 及 AES，且 VPN Throughput 效能至少 2.5 Gbps(含)以上。
7. 設備須能針對加密連線執行 SSL 內容檢測解密功能，並具備網頁加密連線(HTTPS)之解密功能，以提升對資料流之控制與資安防護能力。
8. SSL 加解密需支援 TLS ver 1.2(含以上)並可針對網址、IP 範圍進行加解密 bypass 功能。
9. 支援靜態 IP4 和 IPv6 路由通訊協定(Static Route)以及動態 IPv4 和 IPv6 路由通訊協定 OSPFv2、OSPFv3、BGP 等，具備 USGv6 或 IPv6 Ready Phase 2 等認證。

10. 設備可整合微軟 Active Directory，可動態將使用者 IP（IPv4/IPv6）位址對應至使用者名稱及群組資訊，並以這些資訊做為資安政策之依據
11. 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)
12. 設備可支援虛擬防火牆
13. 支援網路設備 HA (High Availability)： Active-Active / Active-Passive 等備援功能，使單機發生故障無法運作時備援設備接續運作
14. 提供匯出 Netflow v9 資訊，以有效分析資料流，利於管理者根據攻擊發生時間檢視攻擊者或受攻擊者的行為
15. 投標產品設備品牌須通過 NSS Labs NGFW **或** NSS Labs NGIPS 等國際第三方實測安全認證
16. 投標產品設備品牌需為 Gartner Report Network Firewalls 魔術象限領導者
17. 得標廠商須提供設備資安功能防護訂閱授權，須包含入侵防護、應用程式管控、進階惡意程式防護、垃圾郵件過濾、網頁過濾功能、雲端沙箱等
18. 設備需具備 DNS Trap 功能，以強化安全性。
19. 支援匯入第三方情資(Custom feed)與 IoC(Indicator of Compromise)至威脅防禦政策中，可支援 CSV 或 STIX XML 格式，包括 URL、Domain、IP 等形式。
20. 特徵資料庫(Signature Database)需能透過網路更新，須提供三年(含)以上保固，並於保固期內免費提供特徵資料庫更新服務，得標廠商須提供原廠資料庫更新保固証明文件。

（2） 中部、南部新聞中心防火牆及 SSL 加解密系統(共 2 台)

1. 獨立主機採硬體式設備(Hardware Appliance)架構本身提供 **5** 埠(含)以上 1GE RJ45 高速網路連接介面，同時具備 1 埠專屬管理介面。
2. 廠商需提供佐證文件或測試數據，應用程式可辨識 7,000 種(含以上)並當應用程式管控功能開啟的狀態下處理效能 Throughput 須達 **3** Gbps（含)以上。
3. 系統同時連線數至少須達 4 百萬個(含)以上，以及每秒新增連線數須達 60,000 個(含)以上。
4. 廠商需提供佐證文件或測試數據，當防火牆、應用程式控制、入侵防護功能、惡意程式阻絕防護開啟的狀態下，整體處理效能 Throughput 須達 1.5 Gbps（含）以上
5. 具備 IPSec 與 SSL VPN 連線方式，IPSec VPN 加密演算法至少支援 3DES 及 AES 且 VPN Throughput 效能至少 2.7 Gbps（含)以上。
6. 設備須能針對加密連線執行 SSL 內容檢測解密功能，並具備網頁加密連線

(HTTPS)之解密功能，以提升對資料流之控制與資安防護能力。

7. SSL 加解密需支援 TLS ver 1.2(含以上)並可針對網址、IP 範圍進行**加解密** bypass 功能。
8. 支援靜態 IP4 和 IPv6 路由通訊協定(Static Route)以及動態 IPv4 和 IPv6 路由通訊協定 OSPFv2、OSPFv3、BGP 等，具備 USGv6 或 IPv6 Ready Phase 2 等認證
9. 設備內建整合微軟 Active Directory，可動態將使用者 IP（IPv4/IPv6）位址對應至使用者名稱及群組資訊，並以這些資訊做為資安政策之依據
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. 支援網路設備 HA (High Availability)： Active-Active / Active-Passive 等備援功能，使單機發生故障無法運作時備援設備接續運作
12. 提供匯出 Netflow v9 資訊，以有效分析資料流，利於管理者根據攻擊發生時間檢視攻擊者或受攻擊者的行為
13. 投標產品設備品牌須通過 NSS Labs NGFW **或** NSS Labs NGIPS 等國際第三方實測安全認證
14. 投標產品設備品牌需為 Gartner Report Network Firewalls 魔術象限領導者
15. 得標廠商須提供資安功能防護訂閱授權，須包含入侵防護、應用程式管控、進階惡意程式防護、垃圾郵件過濾、網頁過濾功能、雲端沙箱等。
16. 設備需具備 DNS Trap 功能，以強化安全性。
17. 支援匯入第三方情資(Custom feed)與 IoC(Indicator of Compromise)至威脅防禦政策中，可支援 CSV 或 STIX XML 格式，包括 URL、Domain、IP 等形式。
18. 特徵資料庫(Signature Database)需能透過網路更新，須提供三年(含)以上保固，並於保固期內免費提供特徵資料庫更新服務。

（3） B 棟 GSN 防火牆(共 1 台) 30M/30M

1. 獨立主機採硬體式設備(Hardware Appliance)架構本身提供 8 埠(含)以上 1GE RJ45 高速網路連接介面。
2. 廠商需提供佐證文件或測試數據，當應用程式管控功能開啟的狀態下處理效能 Throughput 須達 970 Mbps(含)以上。
3. 系統同時連線數至少須達 500,000 個(含)以上，以及每秒新增連線數須達 15,000 個(含)以上。
4. 具備 IPSec VPN 連線方式，加密演算法至少支援 AES，且 VPN Throughput 效能至少 500 Mbps(含)以上
5. 具備網路位址轉譯(Network Address Translation, NAT)、埠位址轉譯(Port Address Translation, PAT)功能

6. 支援靜態 IP4 和 IPv6 路由通訊協定(Static Route)以及動態 IPv4 和 IPv6 路由通訊協定 BGP、RIP、OSPF 等
7. 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)
8. 具備在 IEEE 802.1q 和 802.3ad 環境下進行防護，並可針對不同 VLAN 套用不同安全政策
9. 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
10. 投標產品設備品牌需為 Gartner Report Network Firewalls 魔術象限領導者

裝

三、 10G 網路交換器

（1） B 棟 10G 網路交換器(2 台)

1. 至少提供 6 埠(含)以上 10 GE SFP+光纖介面
2. 至少提供 1 埠 RJ-45 Serial console port 進行管理
3. Switching Capacity 效能至少需達 228 Gbps(含)以上
4. 系統整體最高可處理 4,000 個(含)以上 VLAN 與 32,768 個(含)以上 MAC 地址
5. 具備 IEEE 802.3ad Link Aggregation(LACP)匯集鏈路能力，支援 8 組 Groups(含)以上
6. 支援 SNMP v1/v2c/v3

訂

四、 L2 1G 網路交換器

線

（1） 中、南部 L2 1G 網路交換器(2 台)

1. 提供 24 埠 10/100/1000Base-T 介面及 4 埠 1000Base-X SFP 介面(可選用 10/100/1000Base-T 或 1000Base-X
2. 至少提供 1 埠 RJ-45 Serial console port 進行管理
3. 整體系統交換容量(Switch Fabric)須達 128Gbps(含)以上，交換能力須達 95 Mpps(含)以上
4. 系統整體最高可處理 256 個(含)以上 VLAN 與 16,000 個(含)以上 MAC 地址
5. 具備 IEEE 802.3ad Link Aggregation(LACP)匯集鏈路能力，支援 8 組 Groups(含)以上
6. 支援 SNMP v1/v2c/v3

五、 防火牆集中化管理平台系統規格

1. 投標廠商得以單一設備或多種軟硬體設備提供下述所有功能，須與本案防火牆產品同品牌以確保最佳支援能力。
2. 可管理本案防火牆並進行集中式網路政策管理、日誌管理與威脅事件分析報表。
3. 日誌管理及報表系統須具備可用硬碟空間至少 6TB (含)以上儲存容量，並支援 RAID 0/1/5/10。
4. 系統提供管理設備數量授權 5 個(含)以上
5. 具備防火牆的安全政策(Policy)集中派送功能
6. 具備防火牆設定版本控管與追蹤功能
7. 具備防火牆韌體版本管理功能，可進行韌體版本更新
8. 具備報表 (Reporting) 管理功能，提供現成的報表樣板，也可依需求客製化報表，報表可自動排程產生，報表格式支援 PDF
9. 具備即時性與歷史日誌資料檢視功能，可依據應用程式、訪問網站、來源位址、目的地位址、資安威脅、管理與系統事件，查看並提供摘要資訊
10. 具備日誌管理功能，需支援日誌排程備份機制，能排程於每日、每週特定時段上傳日誌檔案；支援以 SFTP、SCP、FTP 等方式將日誌檔案傳送至外部伺服器儲存
11. 具備事件告警功能並可以 Email 及 Syslog 等方式發送
12. 系統需提供網頁式管理

六、 網頁應用程式防火牆（共 1 台）

1. 須具備 4 個 1Gbps Gigabit Fiber Ports SFP 連接埠及 2 個 10 Gigabit Fiber Ports SFP+ SLOT 連接埠。
2. 本設備具備 16GB RAM (含)以上。
3. 資料處理能力：

   A) L4 每秒連線處理能力(Connections Per Second)須可達 125,000 connections (含)/秒以上。

   B) L7 每秒需求處理能力(Requests Per Second)須可達 350,000 request(含)/秒以上。

   C) L4/L7 流量處理能力可達 10 Gbps(含)以上。

   D) 最大連接數可達 14,000,000。

4. 內建 SSL 加解密處理能力：

   A) SSL(RSA 2K keys)處理效能(TPS)須達 2,500 transaction/sec（含）以上。

   B) SSL(ECDSA P-256)處理效能(TPS)須達 2,100 transaction/sec（含）以上。

   C) SSL 加密流量須達 5 Gbps（含）以上。

5. 可依服務成長需求，添購授權以擴充原機連線處理能力，無須額外加購設備。
6. 本設備須提供 10 個使用者同時上線透過 SSL VPN 連線。
7. 具備通過 ICSA(International Computer Security Association)之 Web Application Firewall。
8. 具備 OWASP（Open Web Application Security Project）中的以下攻擊手法防禦機制：

   A) 資料隱碼(SQL injection)攻擊與防禦

   B)跨網站攻擊(Cross Site Scripting (XSS))攻擊與防禦

   C)暴力攻擊(Brute Force login)與防禦

   D)參數值之竄改(Parameter Tampering)攻擊與防禦

   E)資訊外洩(Information Leakage)之防範

9. 具備敏感資料保護遮蔽功能，如信用卡號，身份證字號等重要個人資料可進行內容遮蔽並提供 American Express、Diners Club、Discover、JCB、Master Card 及 VISA 之常用金融信用卡資訊之保護。
10. 具備 IP 地理位置資料庫，可根據連線用戶來源 IP 位址，比對地理位址資料庫得知用戶所在地，並依據相關資訊設定安全防禦政策。
11. 具備 AJAX(Asynchronous JavaScript and XML)、JSON（JavaScript Object Notation）辨識防護機制。
12. 具備連線紀錄保留詳細的請求訊息，內容需包含日期、時間、來源 IP、目的 IP、來源埠、目的埠與 HTTP Request 內容。
13. 支援信用交易資料安全標準(PCI DSS)。
14. 具備自動或手動更新安全特徵碼的機制。
15. 具備偵測到入侵攻擊時，提供即時攻擊事件警報(Alert)，並可依電子郵件或 SNMP Trap 或 Syslog 通知系統管理者。
16. 具備偵測特定來源 IP、特定地區或是特定 URL 的請求頻率過高，自動啟用圖形驗證碼(Captcha)機制功能，防止 DoS 攻擊行為。
17. 具備 OWASP TOP 10 的資安漏洞防衛功能及更新。

18. 具備 Cookie 防禦對 Cookie 做加密防止連線被竄改與 Cookie 植入攻擊。
19. 對於自動擷取網站資料的行為加以阻擋。
20. 支援 XML 防火牆功能。
21. 具備 Bot 特徵碼及分類，可針對特定的 Bot 或搜尋引擎進行阻擋。
22. 支援 WebSocket 網路協議。
23. 廠商需提供內建或是外掛 bypass 模組，以防設備異常時保持 Web 對外服務正常運作。

裝

參、 教育訓練

訂

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，並在指定之時間及地點進行教育訓練課程，單項課程至少 4 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 3 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

線

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. 線路及廣域式負載平衡器(至少 2 次)
2. 防火牆暨 SSL 加解密系統（至少 2 次）
3. 防火牆中央控管系統（至少 2 次）
4. 防火牆日誌集中報表系統（至少 2 次）
5. 網頁應用程式防火牆(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
- 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

裝

肆、 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 90 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

訂

線

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

伍、 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，測試通過後始得辦理驗收測試開始為期 60 日曆天內完成，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 7 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	執行要點	備註
1	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	1. 新系統轉移後測試功能 2. 舊系統復原	
3	1. 舊系統復原後測試功能	

陸、 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」、「操作手冊」、「緊急應變手冊」、「災難復原手冊」，並經由公視基金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 2 小時回覆，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

10. 需無償配合本會災難演練、主管機關或行政院之災防演習，需有人力到府。

11. 需無償配合本會依 ISO 27001 之指定的第三方外部稽核或查核，進行實地或書面訪查作業，如有違反資通安全法規情事依合約條款處理，並不得續約。

柒、 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

捌、 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。