資通訊安全防護監控系統、網路傳輸
及終端軟、硬體設施汰換計畫
選擇方案及替代方案之成本效益
分析報告

海洋委員會海巡署

中華民國 112 年 6 月【行政院核定本時間】

資通訊安全防護監控系統、網路傳輸及終端軟、硬體 設施汰換計畫 成本效益分析報告

壹、 辦理依據

- 一、 行政院 108 年 05 月 16 日院臺交字第 1080013437 號函核定。
- 二、 行政院 111 年 04 月 18 日院臺交字第 1110011368 號函核定修正。
- 三、 行政院 112 年 06 月 13 日院臺交字第 1121025333 號函核定修正。

貳、 計畫目標

- 一、 汰換本署資安防護管理中心老舊過時軟、硬體及基礎設施，提升本署資安監控、防禦能量。
改善本署資安防護管理中心(SOC)相關環控、影像監控、不斷電系統等週邊環境設施，並汰換現用老舊防火牆、網頁代理、入侵偵測、防毒軟體、資產管理、修補程式管理、網路監測系統、應用程式防火牆、資安防護管理中心監控系統等軟、硬體資安防護設備，確保整體通資訊系統服務營運效率及全面安全防護。
- 二、 汰換本署及所屬機關廣域及區域網路交換設備，建構高安全性、高延展性及高擴充性巨量資料網路。
為達成資訊安全自動化、即時性及完整性等目標，須建構於高穩定、高可用及高安全性之網路傳輸服務上，始能有效、快速及安全地達成各種外部網路攻擊、各項內部網路使用、終端電腦設備資訊資產存取管控等巨量資料傳輸及分析，考量本署暨所屬各機關單位現行 90 年採購之 53 套骨幹寬頻網路交換設備與各級機關單位內、外網 136 套核心區域網路交換設備(含東、南沙島區節點)老舊，隨著資訊服務向上集中，既有網路系統路由繞送越來越複雜，網路設備必須耗費大量資源拆分或重組傳輸封包，導致傳

輸效率不佳，無法發揮網路頻寬效益，爰規劃汰換相關本署既有 53 套骨幹寬頻網路交換設備及 136 套區域網路設備(含東沙及南沙島區傳輸系統設備)，以建構高安全度、高可用性及具頻寬彈性運用網路，提供網路傳輸層安全防護機制，提升資安防護即時監控、存取管控及事件分析效能。

三、汰換本署及所屬機關單位老舊、防護效能欠佳之伺服器及終端電腦設備，確保營運持續及資訊安全

汰換本署及所屬機關單位至 109 年度使用逾 11 年之資訊應用服務伺服器 86 套、終端個人電腦 1,782 套(終端個人電腦均含作業系統及文書處理軟體)，透過可支援安全性更新之作業系統及硬體效能的升級，同時汰換 1,053 套文書作業軟體(Office)，及可供 15 部雙核心伺服器之微軟 SQL 資料庫作業系統軟體授權(即本案欲採購之 60 套資料庫軟體授權)，以提升終端「點」安裝終端防護基準軟體的效能及伺服器端「面」的管控效能與廣度；另本署現僅有 250 個微軟伺服器企業版裝置用戶端存取使用權及電子郵件伺服器企業版裝置用戶端存取使用權授權，為符合智慧財產權要求，擬籌購微軟伺服器企業版裝置用戶端存取使用權及電子郵件伺服器企業版裝置用戶端存取使用權各 328 套(每套 15 個授權使用數，合計 4,920 個)，以補實本署現有 5583 部資訊電腦及筆記型電腦用戶數之授權需求，提升本署伺服器及終端電腦設備運作之穩定性、有效性及安全性。

參、選擇或替代方案

為因應資安科技日新月異，攻擊手法不斷翻新，需擴大防禦面向廣度，透過專業技術與資源，強化整體資安防禦、偵測與分析告警能量，以確保本署資安防護「面」、網路防衛「線」及終端防禦「點」等面向，及提升整體一元化資安防護能量、海巡網路快速通暢及強化終端設備資訊安全，以因應與日俱增資安

威脅，各項工作均有其必要性，故無替選方案。

肆、財源籌措

本署依據行政院「資訊向上」集中政策，並依據行政院「政府機關（構）資通安全責任等級分級作業規定」資安責任等級 A 級機關應辦事項及 ISMS（ISO27001）遵循事項，為強健本署資安防護能量、網路通連穩定及終端設備可用性，本計畫提報行政院社會發展計畫，本計畫 109 年至 113 年總經費新臺幣 4 億 2,770 萬 2 仟元，109 年度 2,000 萬元、110 年度 9,000 萬元、111 年度 1 億元、112 年度 1 億 7,000 萬元及 113 年 4,770 萬元 2 仟元，各年度所需經費，由公務預算支應。

伍、資金運用

本計畫各工作項目及經費如下：

一、汰換籌補資安防護管理中心(SOC)基礎環境設施暨監控(防護)系統軟、硬體設備：

本資安監控中心採「委外建置、自行營運」方式辦理，且維持運作成功關鍵因素，在於養成專業作業人員，規劃由廠商以技術轉移方式達成，為避免本會海巡署與廠商間技術文件移轉不清、作業流程變更及維護廠商對於系統架構不熟等種種因素，本採購項目擬採「2 年建置（110-111 年）、3 年保固（112 至 114 年）、5 年維護（115 至 119 年）」方式實施，建置(含保固)經費新臺幣 1 億 4,492 萬元。

二、汰換本署暨所屬機關骨幹寬頻網路交換設備：

本採購項目籌建各式網路設備及東、南沙地區網路傳輸系統，並採「4 年(110-113 年)建置、1 年(114 年)保固、5 年(115-119 年)維護」全壽期方式執行，建置(含保固)經費新臺幣 2 億 990 萬元，以一次性招標，分 4 年辦理建置，建置完成後執行 1 年保固並接續 5 年維護，以全壽期系統維運方式招標，吸引專業、殷實廠商進行全壽期規劃與維運。

三、汰換本署及所屬機關至 109 年度預逾使用年限之伺服器、

終端個人電腦及相關軟體授權：

本項目之個人電腦(含液晶螢幕及作業系統)及伺服器(含資料庫軟體)，採行分年採購方式執行，建置(含保固)經費新臺幣 1 億 331 萬元。

陸、成本效益

一、 打造優質機房環境，確保系統正常運作

藉由系統性設計，建置智慧綠能通資訊機房環境基礎設施，可使各式資訊應用系統、資安監控系統及網路傳輸系統等服務均能穩定運作，並提供本署資安防護管理中心(SOC)24 小時全天候監控及管理能量，確保整體通資訊系統服務營運效率。

二、 強化偵測監控機制，即時掌握安全情資

汰換本署資安防護管理中心(SOC)軟(硬)體資安設施，除可有效因應最新資安攻擊技術外，並以集中管控方式，引進最新資料蒐集、偵測、監控及預警等防護，搭配多層式網路層存取管控及終端實體層防毒、系統漏洞修補更新及多媒體存取管控等配套機制，擴大整體資安防禦縱深及威脅數據分析、監控平台資料收容範圍，達成網路節點分區管控、風險範圍控制及有效主動預警及發掘網路異常連線、病毒入侵、駭客攻擊等行為與事件。

三、 建構專屬虛擬網路，強化網路存取管控

汰換本署及所屬機關廣域網路及內、外網區域網路核心交換設備，併納入東沙、南沙與臺灣本島地區網路鏈結，建構本署專屬虛擬網路(VPN)，並搭配 SOC 偵測及網路主動防禦機制，導入流量監控管理、存取管控、服務品質管理(QoS)及可疑網路行為與威脅封鎖，建構高安全度、高可用性及具頻寬彈性運用網路，提供網路傳輸層安全防護機制，以兼顧資訊安全防禦及滿足各級勤(任)務傳輸需求。

四、提升終端防護效能，有效維繫整體安全

個人電腦及伺服器汰換作業至全案 113 年執行完畢後，個人電腦使用逾 11 年(原財產使用年限為 4 年)之比率將從 43%降低至 26%，伺服器使用逾 11 年(原財產使用年限為 4 年)之比率將從 60%降低至 47%，另文書作業及資料庫作業軟體未能獲微軟公司安全性更新比率各別從 61%及 56%降至 28%及 40%，有效提升本署伺服器及終端電腦設備運作之穩定性、有效性及安全性，並滿足各級機關勤(業)務需求，另透過漏洞修補及更新方式降低資訊安全風險，確保機關達成持續營運目標；同時考量政府財政預算有限，引進伺服器虛擬化的技術減少設備數量，降低空間與電力使用量，達到預算樽節及節能減碳政策要求。

五、導入更新組態管理，確保終端環境一致

為降低資通訊設備終端成為駭客入侵管道風險，配合行政院推動政府組態基準 (Government Configuration Baseline) 政策，本署於新基準發布完成測試、評估後，始對所屬終端進行導入佈署及例外管理，惟本署整體資訊終端設備散佈全國各地，數量高達數千部，偶有部分終端發生派送套用失敗狀況，管理者管理不易，故本計畫規劃導入「政府組態基準管控機制」，並配合「程式版本控管、修補(Patch)管理機制」導入，透過群組管理、自動稽核、異常警示等機制，提升終端設備環境管理效率，確保環境一致性，強化終端設備資訊安全強度。

柒、結語

本署海巡署自 109 年執行「資通訊安全防護監控系統、網路傳輸及終端軟、硬體設施汰換計畫」計畫迄今，先後建置新一代基礎環境、佈署資安防禦設備、快速處理海巡網路訊號節點及汰新部分終端設備，提升本會海巡署資安防護「面」、網路防衛「線」及終端防禦「點」等面向，以因應與日俱增資安威脅。