中華民國 109 年 5 月
立法院第 10 屆第 1 會期
經濟、財政、內政、教育及文化、交通、社會福利及衛生環境六委員會第 1 次聯席會議

行政院前瞻基礎建設計畫106至109年績效書面報告

行政院

109 年 5 月 11 日

主席、各位委員：

行政院院本部謹就「強化政府基層機關資安防護及區域聯防計畫」及「強化國家資安基礎建設計畫」106至109年之特別預算編列重點及重要執行成果簡要說明如下：

壹、強化政府基層機關資安防護及區域聯防計畫

一、特別預算編列重點

鑒於國際資安威脅情勢日趨嚴峻，復考量各地方政府因受限經費及人力等因素，甚或有個人電腦或作業系統無維護或更新之狀況，成為政府整體資安防護之高風險所在，為根本解決前述問題、提升國家整體資安防禦能量，本院爰規劃推動「強化政府基層機關資安防護及區域聯防計畫」，以具體強化地方政府資安防護縱深，目前六直轄市政府皆已按規劃逐步建立資安情資分享機制，並持續厚植地方資安防護能量，本計畫重點工作如下：

（一）建構地方政府資安區域聯合防護網，以六

個直轄市政府(臺北市、新北市、桃園市、臺中市、臺南市、高雄市)為核心，結合周邊鄰近縣市推動資安區域聯防體系。

（二）導入政府組態基準(Government Configuration Baseline, GCB)，汰換超過使用年限或停產之資通訊軟硬體設備，以強化地方政府資安端點防護，完備縱深防禦。

二、重要執行成果

（一）推動資安區域聯防機制，具體成效有：

1、建立資安資訊分享與分析中心(Information Sharing and Analysis Center, ISAC)，透過情資格式標準化與系統自動化之分享機制，同步更新惡意中繼站清單及防火牆規則，建立縱向與橫向跨領域之資安威脅與訊息交流，達到情資迅速整合、即時分享及有效應用。

2、建置區域資安威脅預警中心(Security Operation Center, SOC)，並收容鄰近聯防縣市之第一線 SOC，整體機關涵蓋率達 78%；另

透過監控及分析機制獲取資安情資，進行綜合分析以掌握可疑惡意行為，並可派送至端點設備進行防護，有效防止惡意程式擴散。

3、成立資安事件緊急應變機制(Computer Emergency Response Team, CERT)，由各直轄市協調鄰近聯防縣市共同辦理資安事件通報演練，共同研擬各項重大資安事件之緊急應變作為，期能迅速雙向通報及緊急應變處置，並在最短時間內回復，以確保國家利益與政府之正常運作。

(二) 全國 111 個地政事務所(含金門縣、連江縣地政局)啟用數位雙向服務櫃檯，民眾臨櫃申請地籍謄本可免填寫及列印申請書表，環保便民；警政署導入資安專業顧問服務，訓練資安專業人才，進行警政機關資安防護與資安事件防治技術推動與管理，參加 108 年「Red Alert72 資安攻防賽」團隊成員分別獲第 1 名及第 2 名、參加「物聯網設備(IoT)資安挑戰賽」決賽獲得第 4 名及最佳鑑識獎、參加

「HITCON DEFENSE 2019 企業資安攻防大賽」獲得第 2 名。

（三）財政部財政資訊中心規劃五區國稅局網路向上集中網路對外出口，並汰換財政資訊中心及各地區國稅局之老舊伺服主機及網路資安設備，強化稅務平臺作業環境整合及安全，並配合國家發展委員會 T-Road 骨幹網路規劃，建置財政部網路集中出口，強化網路整合管理、增進資源運用、完備縱深防禦，達成資安防護及區域聯防之目標。

（四）汰換基層機關 7 年以上電腦主機及資安防護設備，迄今國內資通訊產品採購金額約 9.6 億元，其中個人電腦採購國產品比例 100%，且已導入政府組態基準設定約有 10 萬臺設備，除強化端點防護及落實資安防護縱深，亦有效活絡我國資訊(安)產業發展。

貳、強化國家資安基礎建設計畫

一、特別預算編列重點

為落實第五期國家資通安全發展方案(106

年至 109 年)所訂之「建構國家安全資安聯防體系」策略，並優先完成能源、水資源、通訊傳播及政府骨幹網路等關鍵基礎設施領域，全面打造數位國家所需之資安聯防基礎建設：

（一）建置政府骨幹網路 SOC 及巨量資料分析平臺，並強化政府機關網域名稱系統(Domain Name System, DNS)服務，達整合分析即時處置，深化防禦縱深能量。

（二）強化水資源關鍵基礎設施資安防護，並建置經濟部 ISAC 及 CERT 平臺，持續擴大納入特定非公務機關，落實聯防機制。

（三）建置國家通訊暨網際安全中心(National Communications and Cyber Security Center, NCCSC)備援中心及網路運作平臺(Network Operation Center, NOC)，以即時掌握重點通訊網路運作狀態，並建置通傳領域 SOC、ISAC 及 CERT，加強通訊網路資安防禦與緊急應變措施。

二、重要執行成果

（一）完成政府骨幹網路 SOC，政府網際服務網(Government Service Network, GSN)之非軍事區(De-Militarized Zone, DMZ)用戶全數導入網頁應用系統防火牆(Web Application Firewall, WAF)防護、本院部會層級全數導入分散式阻斷服務(Distributed Denial of Service, DDoS)攻擊監看防護，提供清洗防護能量；建置臺北、臺中兩套互為異地備援之 Active-Active DNS 系統及相關安全防護，強化高穩定性政府機關 DNS 關鍵基礎服務；巨量資料分析平臺，查找惡意威脅網址，每月平均超過 100 億筆，分析阻擋惡意中繼站，平均每日超過 1 億筆。

（二）完成水資源領域 SOC 及 ISAC 平臺，透過關聯規則對資安監控通報事件進行交叉分析，有效找出資安事件發生原因及研擬防範措施，並持續擴充情資分享來源及範圍；完成經濟部 E-ISAC 及 E-CERT 平臺，並與該部水利署 W-ISAC、能源局民營能源 PE-ISAC、中油公司、

台水公司及台電公司 ISAC 平臺介接。

（三）啟用 NCCSC 異地備援中心，當主中心因天然災害或緊急事故發生造成系統異常時，備援中心可快速且有效率地採取相關必要措施，達到緊急應變與持續營運之目標；NOC 增加六大領域通傳網路業者，迄今已納入 77 家業者(達 85%)；建置通傳領域 SOC、ISAC 及 CERT，累計收容 24 家網際網路接取(IASP)業者，並與 IASP 業者進行雙向自動介接或網頁通報，及持續監控特定漏洞成長情況，迄今超過 25 萬筆。

參、結語

以上為本院主責兩項前瞻基礎建設計畫之重點執行成果，敬請各位委員不吝指教與支持。謝謝！