國家資通安全發展方案(110 年至 113 年)修正對照表

修正內容	現行內容	說明
參、三、資安發展問題評析及應對策略 圖 5 SO 進攻策略「1.建構安全智慧聯網(S1+S2+S3+04)」	參、三、資安發展問題評析及應對策略 圖 5 SO 進攻策略「1.建構智慧國家安全環境(S1+S2+S3+04)」	配合推動策略 4 之具體措施 3「建構安全智慧聯網」修正。 (第 34 頁)
肆、發展藍圖 圖 6 修正為推動策略 4「健全智慧國家資安提升民間防護能量」及其第 3 項具體措施「建構安全智慧聯網」	肆、發展藍圖 圖 6 推動策略 4「建構安全智慧聯網提升民間防護能量」及其第 3 項具體措施「建構智慧國家安全環境」	依策略及措施的範圍合理性，調修內容。 (第 35 頁)
肆、三、推動策略 為培育我國卓越資安人才，精進 CI 防護作為，利用前瞻科技主動防制威脅並溯源阻斷，透由公私協同合作將資安意識與量能普及於民間企業，並健全智慧國家資安，本方案擬具四項推動策略，分別從「吸納全球高階人才、培植自主創研能量」、「推動公私協同治理、提升關鍵設施韌性」、「善用智慧前瞻科技、主動抵禦潛在威脅」及「健全智慧國家資安、	肆、三、推動策略 為培育我國卓越資安人才，精進 CI 防護作為，利用前瞻科技主動防制威脅並溯源阻斷，透由公私協同合作將資安意識與量能普及於民間企業，並建構安全智慧聯網環境，本方案擬具四項推動策略，分別從「吸納全球高階人才、培植自主創研能量」、「推動公私協同治理、提升關鍵設施韌性」、「善用智慧前瞻科技、主動抵禦潛在威脅」及「建構安全智慧聯	配合推動策略 4「健全智慧國家資安、提升民間防護能量」修正。 (第 37 頁)

修正內容	現行內容	說明
提升民間防護能量」等四個面向著手，並配合六大核心戰略產業之「資安卓越產業」規劃持續推動資安產業，期以打造安全堅韌之智慧國家。	網、提升民間防護能量」等四個面向著手，並配合六大核心戰略產業之「資安卓越產業」規劃持續推動資安產業，期以打造安全堅韌之智慧國家。	
肆、三、1.1.1 專案增加師資員額 邀請國內外一流資安競賽團隊、業師、學界和社群知名人士，並提供優渥薪資待遇，以延攬頂尖高階研究人員擔任資安師資，鼓勵大專校院與國內外產業及學研機構競逐優秀資安人才，以利學校培育資安專業人才並維持教學品質。	肆、三、1.1.1 專案增加師資員額 邀請國內外國際一流資安競賽團隊、業師、學界和社群知名人士，並提供優渥薪資待遇，以延攬頂尖高階研究人員擔任資安師資，鼓勵大專校院與國內外產業及學研機構競逐優秀資安人才，以利學校培育資安專業人才並維持教學品質。	酌修文字。 （第 38 頁）
肆、一、(一) 2. 2.1 發展國家任務導向型及關鍵(核心)資安型前瞻研究 因應資安新興威脅及趨勢發展，由資安卓越中心延聘國際優秀人才，負責政府機關短中長期所需之應用技術，以培育並厚植我國資安前瞻研究自主能量。其中國家任務導向型研究，以提供政府機關短中期所	肆、一、(一) 2. 2.1 發展國家任務導向型及關鍵(核心)資安型前瞻研究 因應資安新興威脅及趨勢發展，由資安卓越中心延聘國際優秀人才，負責政府機關短中期所需之應用技術研究，以及國家長期關鍵核心之基礎研究，以培育並厚植我國資安前瞻研究自主能量。	為詳細說明短中期及長期技術研究之定位，爰就國家任務導向型及關鍵(核心)資安型前瞻研究進行說明。 （第 39 頁）

修正內容	現行內容	說明
需之應用技術研究為主，包括技術面及政策面議題；而關鍵核心研究屬長期性基礎型研究，以發展國防、國安之關鍵技術及研究為主。		
肆、三、(一) 2. 2.3 跨國人才交流與研究合作 (1) 參與國際資安標準規範制定，確保開發技術與國際接軌、辦理大型國際學術會議發表研究成果等，藉由國際合作，提升我國國際能見度。	肆、三、(一) 2. 2.3 跨國人才交流與研究合作 (1) 參與國際資安標準規範制定，確保開發技術與國際接軌，並藉由資安前瞻研究成果進行國際合作，提升我國國際能見度。	依據目前資安卓越中心的任務目標，及進行之國際合作活動調整本項內容。(第 39 頁)
肆、三、(三)善用智慧前瞻科技、主動抵禦潛在威脅 鑒於攻擊手法日益精進，傳統防禦已不敷使用，透過情資轉換為有效情報，預測攻擊方式備妥準備，甚至追溯攻擊來源並阻斷等積極防禦手段，以作為我國未來推動重點。本策略以網路攻擊狙殺鏈(Cyber Kill Chain)提出之 7 個攻擊階段：偵查、武裝、遞送、攻擊、安裝、命令與控制、採取行動，制定各個階段之防禦作為。	肆、三、(三)善用智慧前瞻科技、主動抵禦潛在威脅 鑒於攻擊手法日益精進，傳統防禦已不敷使用，透過情資轉換由有效情報，預測攻擊方式備妥準備，甚至追溯攻擊來源並阻斷等積極防禦手段，以作為我國未來推動重點。本策略以網路攻擊狙殺鏈(Cyber Kill Chain)提出之 7 個攻擊階段：偵查、武裝、遞送、攻擊、安裝、命令與控制、採取行動，制定各個階段之防禦作為。	酌修文字。 (第 43 頁)

修正內容	現行內容	說明
肆、發展藍圖 (四) 健全智慧國家資安、提升民間防護能量	肆、發展藍圖 (四) 建構安全智慧聯網、提升民間防護能量	配合推動策略 4「健全智慧國家資安、提升民間防護能量」修正標題。(第 46 頁)
肆、四、機關(單位)分工 表 2 策略四：健全智慧國家資安，提升民間防護能量	肆、四、機關(單位)分工 表 2 策略四：建構安全智慧聯網，提升民間防護能量	配合推動策略 4「健全智慧國家資安、提升民間防護能量」修正。(第 50 頁)
肆、五、(一)培育 350 名資安實戰人才 為因應國家發展之資安人力需求，行政院資安處近年與教育部、科技部、經濟部等機關(單位)共同推動辦理資安專業人才厚植作業，挹注資源以布建資安培育環境，結合國內大學校院資安教學能量，建立以需求為導向之資安人才培訓體系。目前，校園方面已推動資安碩士(學程)班；產業方面，推動產業資安教學及實作課程，發展資安專業訓練及實務應用之人才；國家方面，我國學研機構針對資安前瞻研究部分已完	肆、五、(一)培育 350 名資安實戰人才 為因應國家發展之資安人力需求，行政院資安處近年與教育部、科技部、經濟部等機關(單位)共同推動辦理資安專業人才厚植作業，挹注資源以布建資安培育環境，結合國內大學校院資安教學能量，建立以需求為導向之資安人才培訓體系。目前，校園方面已推動資安碩士(學程)班；產業方面，經濟部針對待業者開設中長期養成班；國家方面，我國學研機構針對資安前瞻研究部分已完成諸多學術研究，逐步建置系統	為詳細說明培育人才於產業面的推動項目，爰調修內容。(第 50 頁)

修正內容	現行內容	說明
成諸多學術研究，逐步建置系統性資安人才培育及前瞻研究制度。	性資安人才培育及前瞻研究制度。	
伍、預期效益 二、面對日益嚴峻的資安威脅環境，將建構主動式防禦機制，於攻擊前透過強化資訊資產弱點管理，並藉由網路及資安防護向上集中，以降低資安風險，達超前部署之效；於攻擊發生時，藉由發展主動式防禦技術，以及深化國內情資綜整平臺，期阻絕攻擊於邊境，達制敵機先之效；最後於攻擊後，持續提升司法單位科技偵查能量，以防制新型網路犯罪，達溯源追蹤之效。再利用資安治理成熟度衡量機制(含客觀指標)，將政府機關之主動防禦能量採量化指標呈現，後續可依衡量結果作為擬訂改善策略之參考，協助機關完善資安基礎環境。	伍、預期效益 二、面對日益嚴峻的資安威脅環境，將建構主動式防禦機制，於攻擊前透過強化資訊資產落點管理，並藉由網路及資安防護向上集中，以降低資安風險，達超前部署之效；於攻擊發生時，藉由發展主動式防禦技術，以及深化國內情資綜整平臺，期阻絕攻擊於邊境，達制敵機先之效；最後於攻擊後，持續提升司法單位科技偵查能量，以防制新型網路犯罪，達溯源追蹤之效。再利用資安治理成熟度衡量機制(含客觀指標)，將政府機關之主動防禦能量採量化指標呈現，後續可依衡量結果作為擬訂改善策略之參考，協助機關完善資安基礎環境。	酌修文字。 (第 54 頁)
柒、附件 1、策略三 1、1-1 推動政府大內網及資安防護向上集中	柒、附件 1、策略三 1、1-1 推動政府大內網及資安防護向上集中	為利更明確推動目標，避免原先以中央 2、3 級機關為

修正內容	現行內容	說明
1、110 年提供至少 6 個 GSN 網路節點具備 SDN 網路架構，以得設置資料中心之機關為單位，完成 80%網路集中出口；完成惡意郵件與網路威脅誘捕向上集中偵蒐機制規劃，並選定 2 個機關試行導入 2、111 年提供至少 10 個 GSN 網路節點具備 SDN 網路架構，以得設置資料中心之機關為單位，完成 90%網路集中出口；推動 2 個機關導入惡意郵件與網路威脅誘捕向上集中偵蒐機制 3、112 年提供至少 15 個 GSN 網路節點具備 SDN 網路架構，以得設置資料中心之機關為單位，完成所有網路集中出口；持續推動 2 個機關導入惡意郵件與網路威脅誘捕向上集中偵蒐機制	1、110 年提供至少 6 個 GSN 網路節點具備 SDN 網路架構，完成 80%中央 2、3 級機關網路集中出口；完成惡意郵件與網路威脅誘捕向上集中偵蒐機制規劃，並選定 2 個機關試行導入 2、111 年提供至少 10 個 GSN 網路節點具備 SDN 網路架構，完成 90%中央 2、3 級機關網路集中出口；推動 2 個機關導入惡意郵件與網路威脅誘捕向上集中偵蒐機制 3、112 年提供至少 15 個 GSN 網路節點具備 SDN 網路架構，完成所有中央 2、3 級機關網路集中出口；持續推動 2 個機關導入惡意郵件與網路威脅誘捕向上集中偵蒐機制	範圍，因部份例外情況致無法達成量化目標，爰修正推動範圍描述。（第 59 頁）
柒、附件 1、策略三 1、1-2 建立資通系統弱點之主動發掘、通報及修補機制 1、110 年 A 級公務機關完成導	柒、附件 1、策略三 1、1-2 建立資通系統弱點之主動發掘、通報及修補機制 1、110 年 A 級公務機關完成導	依資通安全管理法子法之應辦事項要求應導入資安弱點通報機制之期程進行修正。

修正內容	現行內容	說明
入資安弱點通報機制 2、111 年 B 級公務機關及 A、B 級 CI 提供者完成導入資安弱點通報機制 3、112 年 C 級公務機關及 CI 提供者完成導入資安弱點通報機制	入資安弱點通報機制 2、111 年 B 級公務機關及 A 級 CI 提供者完成導入資安弱點通報機制 3、112 年 C 級公務機關及 B 級 CI 提供者完成導入資安弱點通報機制 4、113 年 C 級 CI 提供者完成導入資安弱點通報機制	（第 60 頁）
柒、附件 1、策略三 2、2-1 發展主動式防禦前瞻研究及技術應用 4、113 年研發技術扶植自主研發產品，帶動國內資安/系統整合廠商，支援至少 3 個重點領域(政府、醫療、金融等)，實現資安協作自動化應變技術解決方案(Security Orchestration, Automation and Response, SOAR)；建立 1 套 AI Security 協作產業標準	柒、附件 1、策略三 2、2-1 發展主動式防禦前瞻研究及技術應用 4、113 年研發技術扶植自主研發產品，帶動國內資安/系統整合廠商，達到至少 10 億元產值；建立 1 套 AI Security 協作產業標準	因國內公民營企業採購通常是以資安服務附帶資安產品，營業額非單純商用軟體不易獨立計算產值，且國內市場仍在推廣使用 AI 資安偵防產品，評估 10 億元產值有調查統計上的困難度，另考量法人研發資安關鍵技術，係以協助廠商提升產品品質與服務擴散各產業為主軸，爰調修量化目標。(第 60 頁)
柒、附件 1、分年重要進程	柒、附件 1、分年重要進程	配合推動策略 4

修正內容	現行內容	說明
策略四：健全智慧國家資安，提升民間防護能量	策略四：建構安全智慧聯網，提升民間防護能量	「健全智慧國家資安、提升民間防護能量」修正標題。（第 62 頁）
柒、附件 1、策略四 2、2-2 聚焦資通訊晶片產品安全性 2、111 年研發晶片旁通道攻擊檢測自動化工具 1 套；成立國內晶片安全檢測實驗室；協助至少 2 家國內晶片業者之晶片產品通過晶片安全測試相關標準，發行晶片安全測試報告 3、112 年研發矽前旁通道弱點模糊測試工具 1 套；晶片安全檢測實驗室取得國際認可；協助至少 2 家晶片業者之晶片產品進行場域安全實證	柒、附件 1、策略四 2、2-2 聚焦資通訊晶片產品安全性 2、111 年研發晶片旁通道攻擊檢測工具 1 套；成立國內晶片安全檢測實驗室；協助至少 2 家晶片業者進行晶片安全檢測工具場域實證 3、112 年研發惡意邏輯加速模糊測試工具 1 套；晶片安全檢測實驗室取得國際認可；協助至少 2 家晶片業者進行晶片安全檢測工具場域實證	因「晶片惡意邏輯檢測」及「晶片旁通道攻擊檢測」應有延續性，4 年做到具競爭力的商用技術，並考量旁通道攻擊的檢測，急需自動化與智慧化檢測技術支援取代人工判斷，爰整合並調修 111 年、112 年工作目標。（第 63 頁）
柒、附件 1、策略四 3、3-2 推動物聯網合規驗證及場域實證 1.110 年制定我國物聯網資安檢測驗證框架，並於111 年擬訂物聯網資安標準優先制定策	柒、附件 1、策略四 3、3-2 推動物聯網合規驗證及場域實證 1.110 年制定我國物聯網資安檢測驗證框架，並於 111 年擬訂物聯網資安檢測優先策略及	因物聯網資安標準制定才有優先順序的策略及清單擬定，檢測係依標準進行，爰調修內容，並刪除第 2 點的「指標」用語，

修正內容	現行內容	說明
略及清單項目 2.每年建立1項應用示範展示場域，涵蓋至少2項次資安技術或產品應用；111年起每年促成1案次創新資安技術或產品試煉應用實證	清單項目 2.每年建立1項指標應用示範展示場域，涵蓋至少2項次資安技術或產品應用；111年起每年促成1案次創新資安技術或產品試煉應用實證	以符合原意。 （第63頁）