檔　　號:
保存年限:

行政院資通安全處 函

地址：10058 臺北市忠孝東路1段1號
傳真：(02)2397-3457
聯絡人：史凱文(02)3356-6500#8351
電子信箱：kwshih@ey.gov.tw

受文者：臺南市政府

發文日期：中華民國111年8月10日
發文字號：院臺護字第1110183357D號
速別：普通件
密等及解密條件或保密期限：
附件：中央政府前瞻基礎建設計畫第4期特別預算案「政府基層機關資安主動防禦計畫」經費補助彙整表（請至 http://attachment.ey.gov.tw 下載，下載識別碼：2754）（1110183357D-0-0.pdf）

主旨：檢送「中央政府前瞻基礎建設計畫第4期特別預算案(112年度及113年度)」項下「政府基層機關資安主動防禦計畫」經費補助彙整表1份，請查照。

說明：旨揭補助經費後續仍須經立法院審議，如有調整，將另行通知。

正本：臺南市政府、雲林縣政府、嘉義市政府、嘉義縣政府
副本：電子公文交換章 2022/08/10 13:48:33

「中央政府前瞻基礎建設計畫第4期特別預算案(112年度及113年度)」項下

「政府基層機關資安主動防禦計畫」經費補助彙整表

單位：新臺幣元

地方政府	補助比例	112年度				113年度			
		估列分配數				估列分配數			
		估列分配數	補助總額	補助經常門	補助資本門	估列分配數	補助總額	補助經常門	補助資本門
臺南市	70%	36,893,914	25,825,740	9,400,100	16,425,640	45,937,571	32,156,300	7,793,500	24,362,800
嘉義市	70%	7,250,000	5,075,000	3,500,000	1,575,000	0	0	0	0
嘉義縣	90%	11,600,000	10,440,000	9,990,000	450,000	23,555,556	21,200,000	13,100,000	8,100,000
雲林縣	80%	36,570,925	29,256,740	5,678,000	23,578,740	14,035,550	11,228,440	0	11,228,440

臺南市政府112至113年度前瞻基礎建設

政府基層機關資安主動防禦計畫

一、 計畫緣起

因應行政院辦理112至113年度前瞻基礎建設「強化政府基層機關資安防護計畫」，推動資訊資源向上集中，持續強化資安防護能量，推動滲透測試及紅藍軍攻防演練。考量區域縣市所屬一級機關、二級機關及公所，機關總數眾多為降低基層機關承擔獨自連網之資安風險，推動政府資訊資源向上集中，擬辦理府外單位線路整併及建立完善之共用資料中心，強化資安端點防護，落實資訊系統弱點通報機制，並培訓資安人才及推動紅藍隊演練或資安檢測，期能有助於帶動資安產業發展，爰訂本計畫。

二、 計畫目標

本計畫規劃以「推動資訊資源向上集中」、「精進資安防護能量」及「推動滲透測試及紅藍軍攻防演練」為三大主軸，並以「強化政府基層機關、精進資安防護能力」為基礎，研提資安創新服務，以期達成「安全可信賴之資訊資源集中共享環境」之願景。

(一) 資訊資源向上集中

建置共用資料中心，整併本市所屬6個外部單位資訊機房資源。

(二) 精進資安防護能量

精進資安防護能量，導入8個C級機關VANS、6個B級機關EDR。

(三) 推動滲透測試及紅藍軍攻防演練

結合沙崙資安大樓實證場域，辦理攻防演練及資安人才培育。

三、 計畫內容與實施策略

(一) 資訊資源向上集中

1. 成立「資訊資源向上集中」專案輔導建置團隊：
   進行本府所屬機關資訊資源向上集中之推廣及整併作業　。
2. 整併網路：辦理本市所屬6個外部單位資訊機房VPN線路建置及收容。
3. 建置共用資料中心：

（1） 整併本市所屬 6 個外部單位資訊機房至本府資料中心。

（2） 辦理機房整併規劃、空間與結構設計、電力、空調、消防、環控系統建置、雲端運算資源擴充。

（3） 辦理 200 個資訊系統移轉、虛擬機移轉、管理平台建置、資料備份管理、系統效能監控、系統異常告警、系統軟體授、系統日誌管理。

4. 建置及推廣共用性系統

建置「共用目錄服務系統」，推廣本市所屬機關學校使用。

（二）精進資安防護能量

1. 推動導入資訊系統弱點通報機制 VANS（8 個 C 級機關）。
2. 推動導入建立端點威脅偵測及應變機制 EDR（6 個 B 級機關）。
3. 建立資產盤點系統。

（三）推動滲透測試及紅藍軍攻防演練

1. 結合沙崙資安大樓實證場域辦理紅藍隊攻防演練每年一次或資安滲透檢測系統至少 5 案。
2. 培訓紅藍隊資安攻防人才至少 35 人次。

四、 實施範圍

有關本計畫實施對象及實施區域，線路整併本市 6 個外部單位資訊機房，建置共用資料中心預計辦理 200 個虛擬機系統整併、移轉作業，及推動各項共用系統導入及資安防禦工作，詳細說明如下：

策略面向	工作項目	實施對象	實施區域
資訊資源向上集中	整併網路線路	本市所屬各級機關	本市所屬 6 個外部單位資訊機房 VPN 線路建置
	建置共用資料中心	本市所屬各級機關	整併本市所屬 6 個外部單位資訊機房至本府資料中心，辦理 200 個資訊系統移轉作業，預計 2 年計畫中，每年辦理約 3 個資料中心減量，及每年辦理約 100 個資訊系統移轉作業。

	建置及推廣共用性系統	本市所屬各級機關	建置「共用目錄服務系統」，推廣本市所屬機關學校使用
精進資安防護能量	導入資訊系統弱點通報機制(VANS)	本市所屬責任等級C級機關	推動本府3000U包含所屬8個資安責任等級C級機關導入VANS。
	導入端點偵測及應變機制(EDR)	本市所屬責任等級B級機關	推動本府4900U包含所屬6個資安責任等級B級機關導入EDR。
推動滲透測試及紅藍軍攻防演練	辦理紅藍隊攻防演練及資安檢測	本市永華、民治雙市政中心、沙崙資安暨智慧科技研發大樓	結合沙崙資安大樓實證場域辦理紅藍隊攻防演練每年一次或資安滲透檢測系統至少5案。
	資安人才培育	本市所屬各級機關	培訓紅藍隊資安攻防人才至少15人次

五、 計畫期程

112年1月1日至113年12月31日。

六、 關鍵績效指標及年度目標值

年度	項次	關鍵績效指標	目標值
112	1	完成資料中心減量個數	3
	2	完成資訊系統資源佈署個數	100
	3	資通安全責任等級C級機關導入介接VANS導入數	8
	4	資通安全責任等級B級機關導入EDR導入數	3

	5	推動紅藍隊攻防演練次數(或資安檢測至少 3 案)	1
	6	培訓紅藍隊資安攻防人才人次	15
113	1	完成資料中心減量個數	3
	2	完成資訊系統資源佈署個數	100
	3	資通安全責任等級 B 級機關提交 EDR 至主管機關指定位置提交數	6
	4	推動紅藍隊攻防演練次數(或資安檢測至少 5 案)	1
	5	培訓紅藍隊資安攻防人才人次	20

七、 持續營運評估

本計畫期程結束後，後續維運方式擬由本府各機關年度編列預算辦理系統維運、網路線路租用、軟體授權及攻防演練經費維持等，細部評估表如下：

項次	策略面向	工作項目	後續維運服務模式	後續維運經費評估
1	資訊資源向上集中	整併網路線路	線路費及設備維護	由各使用機關每年編列預算維護： 網路線路租用費用，每年每單位約 30 仟元。網路設備維護費約原購置經費 15%，每年每單位約 150 仟元。
2		建置共用資料中心	系統維運	由本府每年編列預算維護： 系統租賃維運費 200 個虛擬系統，約 6000 仟元。
3		建置及推廣共用性系統	系統維運	由本府每年編列預算維護： 設備及系統維運費約原購置經費 15%，約 1000 仟元。
4	精進資安防護能量	導入資訊系統弱點通報機制	系統授權及維護	由本府各使用機關每年編列預算維護：

		(VANS)		每年系統授權及維護費用，每年約3,480仟元。
5		導入端點偵測及應變機制(EDR)	系統授權及維護	由本府各使用機關每年編列預算維護： 每年系統授權及維護費用，每年約11,600仟元。
6	推動滲透測試及紅藍軍攻防演練	辦理紅藍隊攻防演練及資安檢測	持續維持	由本府每年編列預算持續維持，約1,000仟元。
7		資安人才培育	持續維持	由本府每年編列預算持續維持，約1,000仟元。

八、 經費明細概算

年度	項次	工作項目	工作內容	所需經費		績效目標	優先次序
				經常門	資本門		
112	1	資訊資源向上集中	辦理本市所屬3個外部單位資訊機房VPN線路整併。	1,500,000	1,500,000	整併本市3個外部單位資訊機房線路設備。	1
			建置共用資料中心 1. 辦理機房整併前置規劃、空間與結構設計、電力、空調、消防、環控系統建置、雲端運算資源擴充。 2. 完成100個資訊系統資源佈署、虛擬機移轉、管理平台建置、資料備份管理、系統效能監控、系統異常告警、系	6,628,714	7,615,200	建立本市資料中心，並完成100個資訊系統資源佈署。	4

			統軟體授、系統日誌管理。				
	2	精進資安防護能量	推動本府 3000U 包含所屬 8 個資安責任等級 C 級機關導入 VANS。	3,300,000	4,350,000	導入 VANS 至 8 個 C 級機關。	2
			推動本府 2000U 包含所屬 3 個資安責任等級 B 級機關導入 EDR	0	10,000,000	導入 EDR 至 3 個 B 級機關。	3
	3	推動滲透測試及紅藍軍攻防演練	推動紅藍隊攻防演練每年一次或資安滲透檢測系統至少 3 案	1,000,000	0	推動紅藍隊攻防演練每年一次或資安檢測至少 3 案	5
			培訓紅藍隊資安攻防人才至少 15 人次	1,000,000	0	培訓紅藍隊資安攻防人才至少 15 人次	6
小　　計				13,428,714	23,465,200		
合　　計				36,893,914			

年度	項次	工作項目	工作內容	所需經費		績效目標	優先次序
				經常門	資本門		
113	1	資訊資源向上	辦理本市所屬 3 個外部單位資訊機房 VPN 線路整併。	1,500,000	1,500,000	整併本市 3 個外部單位資訊機房線路設備。	1

		集中	建置共用資料中心 1. 辦理機房整併前置規劃、空間與結構設計、電力、空調、消防、環控系統建置、雲端運算資源擴充。 2. 完成 100 個資訊系統資源佈署、虛擬機移轉、管理平台建置、資料備份管理、系統效能監控、系統異常告警、系統軟體授、系統日誌管理。	6,633,571	13,604,000	建立本市資料中心，並完成 100 個資訊系統資源佈署。	3
			建置及推廣共用性系統	0	5,200,000	完成共用系統建置。	4
	2	精進資安防護能量	推動本府 2900U 包含所屬 3 個資安責任等級 B 級機關導入 EDR	0	14,500,000	導入 EDR 至 3 個 B 級機關。	2
	3	推動滲透測試及紅藍軍攻防演練	推動紅藍隊攻防演練每年一次或資安滲透檢測系統至少 5 案	1,500,000	0	推動紅藍隊攻防演練每年一次或資安檢測至少 5 案	5
			培訓紅藍隊資安攻防人才至少 20 人次	1,500,000	0	培訓紅藍隊資安攻防人才至少 20 人次	6
小　　計				11,133,571	34,804,000		
合　　計				45,937,571			

九、 經費補助表

單位：新臺幣元

年度	總經費	其他基金或補助款	地方政府自籌款	行政院補助款
112年	36,893,914	0	11,068,174	25,825,740
113年	45,937,571	0	13,781,271	32,156,300

十、 預定進度

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
112/6	27%	10,000,000	推動本府所屬 3 個資安責任等級 B 級機關導入 EDR 2000U（第 1 期）
112/10	48%	17,650,000	推動本府所屬 8 個資安責任等級 C 級機關導入 VANS 3000U
112/10	56%	20,650,000	完成本市 3 個外部單位資訊機房 VPN 線路整併(第 1 期)
112/10	95%	34,893,914	完成 100 個資訊系統資源佈署(第 1 期)
112/12	97%	35,893,914	辦理紅藍隊攻防演練及資安檢測(第 1 期)
112/12	100%	36,893,914	培訓紅藍隊資安攻防人才(第 1 期)

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
113/6	32%	14,500,000	推動本府所屬 3 個資安責任等級 B 級機關導入 EDR 2900U（第 2 期）

113/10	38%	17,500,000	完成本市 3 個外部單位資訊機房 VPN 線路整併(第 2 期)
113/10	82%	37,737,571	完成 100 個資訊系統資源佈署(第 2 期)
113/12	93%	42,937,571	建置及推廣共用性系統
113/12	97%	44,437,571	辦理紅藍隊攻防演練及資安檢測(第 2 期)
113/12	100%	45,937,571	培訓紅藍隊資安攻防人才(第 2 期)

十一、預期效益

項次	工作項目	預期效益
1	整併網路線路	1. 整併所屬機關網路線路，建構完整網路集中資源架構。 2. 有效管理網路資源，提升基層機關資安防護能力。
2	建置共用資料中心	1. 完備政府雲端服務發展環境，深化資訊系統雲端化服務量能。 2. 有效運用有限資源以避免過於分散，提升機房可用性及能源運用效率。 3. 資訊資源統籌管理，建構完整資訊安全防護控管。
3	建置及推廣共用性系統	建置共用電子郵件系統，並推廣本市所屬 392 個機關學校使用。 以容器虛擬化技術為主的虛擬化私有雲平台，為核心共通系統整併/重構/再利用、政府數位化進程（系統化、服務化、自動化、智慧化）奠定基礎。
4	導入資訊系統弱點通報機制(VANS)	1. 落實資通安全管理法之資產盤點、風險評估應辦事項。 2. 有效管理市府資訊資產。 3. 與行政院技術服務中心 VANS 系統合作，取得資訊資產弱點清單，避免重複建置。 4. 強化資訊資產弱點管理：因近年系統使用開源軟體、框架、套件及模組日漸普遍，此類套件並未落入傳統弱點掃描範圍內。透過資訊資產盤點可將其納入，達到有效控管並持續追蹤。

5	導入端點偵測及應變機制(EDR)	1. 佈署內網端點威脅防禦系統，採系統行為分析方式進行端點威脅偵測，自動關聯資安事件發生之主要原因與軌跡。 2. 輔助防毒軟體採特徵值防護之不足，並加速採證及資安鑑識作業。
6	辦理紅藍隊攻防演練及資安檢測	1. 進行紅藍隊攻防演練或資安檢測，提高機關的資安防護能量。 2. 針對所有發現漏洞及防護瑕疵，提出風險報告與建議改善措施。
7	資安人才培育	辦理產官學研合作，結合 EDR 及事件應變流程，將惡意檔案進行逆向工程分析，並將其經驗及案例融入至訓練教材，藉由實務經驗與案例來培養資安人材。

十二、相關聯絡資料

機關單位	姓名	電話	E-mail
臺南市政府智慧發展中心	邱文志	06-3901481	itel41@mail.tainan.gov.tw
臺南市政府智慧發展中心	洪將涵	06-2991111#8060	chhung@mail.tainan.gov.tw
臺南市政府智慧發展中心	李佳璋	06-3901181	splay@mail.tainan.gov.tw