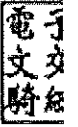


行政院秘書長 函

地址：10058臺北市忠孝東路1段1號
聯絡人：戴全裕(02)33568068
電子信箱：cytai@ey.gov.tw



受文者：臺南市政府

發文日期：中華民國110年7月20日

發文字號：院臺護長字第1100179621D號

速別：普通件

密等及解密條件或保密期限：

附件：如主旨 (1100179621D-0-0.docx、1100179621D-0-1.pdf)

主旨：檢送「強化政府基層機關資安防護計畫」核定補助經費表及審核意見表各1份，請依說明四辦理，請查照。

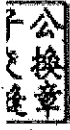


說明：

- 一、旨揭計畫補助經費已於本(110)年6月28日經本院國家科學技術發展基金(以下簡稱科發基金)管理會核定。
- 二、鑒於科發基金本年度預算尚未通過，後續法定預算審議結果如有刪減，本院保留調整核定金額之彈性。
- 三、為帶動我國資通安全產業發展及強化國家資通安全防護能量，本計畫採購之軟硬體設備優先以國內自主產品為主，因故無法採用國內自主產品，應簽報機關首長同意後副知本院，無須經本院同意，惟本院仍將國內自主產品之使用比例納入未來補助參考。
- 四、請依據計畫核定補助經費額度及審核意見表修正貴府共同提報之「強化政府基層機關資安防護計畫」，並於文到後一週內函復，另後續經費補助事宜請依本院訂定「行政院補助地方政府強化資通安全防護作業要點」辦理。

正本：臺南市政府

副本：雲林縣政府、嘉義縣政府、嘉義市政府(均含附件)



裝

訂

線

「強化政府基層機關資安防護計畫」核定補助經費表

地方 政府	財力 分級	補助 比率	地方政府 送審數	核定數	本院補助總額 (核定數*補助比率)	本院補助 經常門	本院補助 資本門
臺南市	第三級	70%	54,847	54,847	38,393	9,812	28,581

單位：千元

審核意見表

計畫名稱	強化政府基層機關資安防護計畫		
主管/規劃機關	行政院資通安全處	執行機關	行政院資通安全處

審查意見

- (一)計畫除編列預算協助導入資安弱點通報機制外，後續要如何瞭解其運作的狀況與有效性，應規劃檢驗及稽核機制。
- (二)對於地方基層欠缺資安人才之議題應有配套規劃與投入。
- (三)對於「精進資安防護能量」項目之建議：各地方政府所轄之資安防護能力(技術與人力)不一，宜加強督導，並協助防護力較弱的縣市完善其推動策略。
- (四)對於「資訊資源向上集中」項目之建議：
1. 虛擬化技術與網路整併技術之建立為「我國正發展中之產品或技術」，各縣市計畫書(整併成6區)中所述之作法不一，且部分技術並未真正融入推動事項中，應加強督導。
 2. 建置共用資料中心及推廣共用性系統，這是將分散式系統集中化的措施，必須要注意 single-point of failure 的問題，至少應有異地備援機制，然檢視六都目前計畫內容僅規劃資料備份，有所不足。
 3. 計畫建置及推廣共用性系統，應規劃定期瞭解地方機關使用狀況及滿意度等指標。
 4. 計畫擬產出資訊資源向上集中先期規劃報告，提供地方政府進行資訊資源向上集中化作業的參考依據。考量計畫推動之時程及品質，建議在各區建置前，宜完成此報告並經第三方公正單位評估其適切性及可擴充性。
- (五)推動政府機關導入介接 VANS，建議於各縣市及各區介接完成後，進行「不定時」實務演練，以確保系統及資訊資料之可用性。並應建立 VANS 常見問題 Q&A 網站，對相關地方機關人員進行培訓或教育訓練，以確保計畫之順利執行。
- (六)所列各縣市自籌款偏低，提案單位宜請各縣市逐年增加資安相關預算之投入。
- (七)後續導入需更積極方可確保 C 級機關可在資安法修正施行後 2 年內完成導入 VANS 作業，以合乎法規。
- (八)對主要績效指標之意見如下：
1. 目前有研究報告 6 篇，並著眼於降低因資訊資源向上集中未事先規劃導致服務中斷風險，建議應強化資訊資源向上集中的資安防護架構，如零信任網路佈署、共通出口的 DDoS 防護、APT 防護、共同資安情資…等。
 2. 目前績效指標是 100 個 B 級以上機關導入 VANS，但導入 VANS 的目的是「縮短或最小化資訊資產弱點曝險的時間」，所以減少曝險時間才是績效指標。應思考把「做好好」納入績效指標，例如，「對於已發現或公告的重大弱點(CVSS 定義為 Critical or High)，應於三天內偵測、通報到給相關人員，並於六天內完成修補」。
 3. 請具體回復說明新增之績效指標「B 級機關收到 CVSS 7 分以上之弱點通報，評估須修復者，未於通報後 1 個月內完成修復之機關比例小於 30%」。
 4. 各量化指標於計畫推動前應讓參與推動之各地方政府知悉(如地方政府資通安全責任等級 B 級以上機關導入介接 VANS 機制導入率達 100%)。
 5. 減量、縮減及整併之量化指標於再依不同區或縣市現況而賦予不同之目標，以利各縣市或區依循。

審查意見

6. 聯防具體策略作為應明述，並有對應 KPI，且 KPI、達成政策評估、年度里程碑等宜於執行時強化。

(九)建議在計畫最後一個月進行系統介接之成果實測演練，並評估其弱點通報及修補之成果與效率。

(十)建議規劃單位科技會報辦公室應定期落實成效追蹤。

臺南市政府 110 年度強化基層機關資安防護計畫

一、計畫緣起

本府因應行政院辦理「強化政府基層機關資安防護計畫」補助，推動資訊資源向上集中，持續強化資安防護能量及端點防護，辦理外網線路整併及建立完善之共用資料中心，創新建置資安視覺化儀表板，降低本府所屬基層機關承擔獨自連網之資安風險，爰訂本計畫。

二、計畫目標

本計畫規劃以「資訊資源整併」及「資訊服務共享」為兩大主軸，並以「強化政府基層機關、精進資安防護能力」為基礎，以期達成「安全可信賴之資訊共享環境」之目標。

● 計畫亮點 1：建置共用資料中心，成立專案輔導團隊。

(一)建置共用資料中心，提供 250 台虛擬機資源，整併本市所屬 37 個區公所資訊機房，辦理線路集中及資安設備收容，強化網路資安整體架構；亦成立專案導團隊，建立計畫執行常見問題 Q&A 網站，協助本府基層機關瞭解資源向上集中之政策目標及配合事項。

(二)建置推廣國發會「ODF 在地雲端共用空間系統」，與市政公務入口網進行單簽介接，導入 5000 個公務帳號，並要求所屬機關資料儲存禁止使用公有雲端磁碟空間，避免重要公務資料外流。

● 計畫亮點 2：佈署基層端點防禦，精進資安防護能量。

依行政院資安政策，推動本府所屬資安責任等級 B 級機關，全面導入 VANS 資訊系統弱點通報系統，強化端點防護，並推動 VANS 弱點通報工作項，納入現行 ISAC 區域聯防機制，並不定時辦理實務演練，以確保系統及資訊資料之可用性。

協同雲嘉嘉南區域聯防四縣市，共同建置「主機/網站弱掃共通管理平台」，每季辦理 250 個以上之主機及網站弱點掃描，並主動郵件通知系統管理者修補漏洞，定期追蹤高風險漏洞修補情形，落實檢驗及稽核機制，並完整保存歷史紀錄供後續分析參考。

● 計畫亮點 3：研提自動化創新服務，建立視覺化儀表板。

建置 VANS 弱點修補系統，整合端點防護軟體資訊蒐集，採自動化方式與中控台強制報到修補，降低零時差惡意探索被攻擊之風險。

透過串接 API 整合弱點修補數據，建立視覺化儀表板，呈現端點設備、伺服器主機、系統網站弱點修補情形。

三、計畫內容與實施策略

- 資訊資源向上集中：

- 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，並完成「資訊資源向上集中之中、長期規劃報告」，盤點各項資訊服務潛在資安風險，強化資訊資源向上集中之資安防護整體架構。

- 整併網路：

- 辦理本市所屬 37 個區公所 VPN 線路建置及收容約 3000 台個人電腦。

- 建置共用資料中心：

- A. 整併本市所屬 37 個區公所資訊機房至本府資料中心。

- B. 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。

- C. 建立 250 台虛擬機資源，並辦理資訊系統移轉、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、系統日誌管理等工作。

- 建置及推廣共用性系統：

- 建置推廣國發會「ODF 在地雲端共用空間系統」，提供 100GB × 5000 個帳號供本府所屬機關同仁使用，並要求所屬機關禁止使用公有雲端空間進行公務檔案資料存取。

- 建置主機/網站弱掃共通管理平台：

- 協同雲嘉嘉南區域聯防四縣市，共同建置「主機/網站弱掃共通管理平台」，每季辦理 250 個以上之主機及網站弱點掃描，並即時將弱掃結果以視覺化方式呈現，並主動郵件通知系統管理者修補漏洞，並定期追蹤高風險漏洞修補情形，落實檢驗及稽核機制，並完整保存歷史紀錄供後續分析參考。

- 精進資安防護能量

- 推廣 VANS：

- 推動本府 4,500U 包含所屬 6 個資安責任等級 B 級機關導入 VANS，並建立 VANS 弱點修補系統，整合端點防護軟體資訊蒐集，自動與中控台強制報到修補，降低零時差惡意探索被攻擊之風險，同時推動 VANS 弱點通報工作項，納入現行 ISAC 區域聯防機制，並不定時辦理實務演練，以確保系統及資訊資料之可用性。

- 建立視覺化儀表：

- 並建立視覺化儀表板，呈現端點設備、伺服器主機、系統網站弱點修補情形。

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 37 個區公所，共用資料中心預計建置 250 個虛擬機資源，並辦理系統整併、移轉作業，及推動各項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	本市永華、民治雙市政中心暨所屬各區公所	本市所屬 37 個區公所 VPN 線路建置
	建置共用資料中心	本市永華、民治雙市政中心暨所屬各區公所	整併本市所屬 37 個區公所資訊機房至本府資料中心，建置 250 個虛擬機資源，並辦理資訊系統移轉作業相關作業。
	建置及推廣共用性系統	本市所屬各級機關及各區公所 雲嘉嘉南區域聯防四縣市	辦理所屬機關終端電腦收容管理，採購 AD 3000U 授權。 建置推廣國發會 ODF 在地雲端共用空間系統，提供本市 100GB×5000 個公務帳號使用。 協同雲嘉嘉南區域聯防四縣市，共同建置「主機/網站弱掃共通管理平台」，每季辦理 250 個以上之主機及網站弱點掃描。
精進資安防護能量	推廣 VANS	本市永華、民治雙市政中心暨所屬責任等級 B 級機關	推動本府 4,500U 包含所屬 6 個資安責任等級 B 級機關導入 VANS。

五、計畫期程

民國 110 年 7 月至 111 年 6 月。

六、關鍵績效指標及年度目標值

項次	績效指標	目標值
1	資訊機房減量數	37 個區公所（召開 2 場次說明會）、完成「資訊資源向上集中之中、長期規劃報告」1 份
2	資料共用中心虛擬機整併數	250 個虛擬機（含所屬各級機關、區公所資訊系統）
3	收容終端點電腦	3000 台個人電腦（區公所電腦） 建置作業系統自動更新及修補服務(WSUS)，提供至少 900 台電腦及主機使用
4	推動共用性系統數	2（建置國發會 ODF 私有雲端共用空間系統，提供 5000 個公務帳號，辦理 8 場教育訓練，及區域聯防「主機/網站弱掃共通管理平台」）。

5	精進資安防護資安責任等級 B 級機關 VANS 導入率	100% (推動所屬 6 個 B 級機關：4500U)
6	視覺化儀表版數	1 (建置「本市端點設備弱點情形儀表板」)

七、經費明細概算

單位：新臺幣元

績效目標	項次	工作項目	工作內容	所需經費		優先次序
				經常門	資本門	
資訊資源向上集中	1	整併網路線路	1. 成立「資訊資源向上集中」專案輔導建置團隊，並完成「資訊資源向上集中之中、長期規劃報告」1 份。 2. 辦理本市所屬 37 個區公所 VPN 線路佈署，及防火牆/路由設備建置。	6,217,000	2,500,000	2
	2	建置共用資料中心	1. 辦理機房整併前置規劃(包含：機房空間、電力、空調、環控及運算資源)。 2. 整併本市所屬 37 個區公所資訊機房至本府資料中心。 3. 建置本府資料中心 250 個虛擬機資源，並辦理資訊系統移轉、管理平台建置、資料備份管理、系統效能監控、系統異常告警、系統日誌管理等工作。	2,000,000	24,830,000	3
	3	建置及推廣共用性系統	1. 辦理所屬機關終端電腦收容管理，採購 AD 3000U 授權。 2. 建置推廣 ODF 在地雲端共用空間系統，100GBx5000 個帳號。 3. 協同雲嘉嘉南區域聯防四縣市，共同建置「主機/網站弱掃共通管理平台」，每季辦理 250 個	0	13,300,000	4

			以上之主機及網站弱點掃描，並即時將弱掃結果以視覺化方式呈現，並主動郵件通知系統管理者修補漏洞。			
導入 VANS	4	推廣 VANS	1. 推動本府 4500U 包含所屬 6 個資安責任等級 B 級機關導入 VANS。 2. 推動 VANS 弱點通報工作項，納入現行 ISAC 機制。 3. 建立視覺化儀表板，呈現端點設備弱點情形。	5,800,000	200,000	1
小計				14,017,000	40,830,000	
合計					54,847,000	

八、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	行政院資通安全處補助款
110	54,847,000	0	16,454,000	38,393,000

九、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	1. 建置推廣國發會 ODF 在地雲端共用空間系統，100GBx5000 個帳號，提供所屬機關資料儲存空間，禁止使用公有雲端磁碟空間，減少重要公務資料外流情事發生。 2. 建置「主機/網站弱掃共通管理平台」，每季辦理主機及網站弱點掃描，並即時將弱掃結果以視覺化方式呈現，並主動郵件通知系統管理者修補漏洞，定期追蹤高風險漏洞修補情形，落實檢驗及稽核機制，並完整保存歷史紀錄供後續分析參考。
4	推廣 VANS	1. 落實資通安全管理法之端點設備弱點資訊盤點、風險評估應辦事

		<p>項。</p> <p>2. 結合行政院技術服務中心 VANS 系統，即時取得資訊資產弱點清單，通知系統管理者派送修補規則，或通知使用者修補漏洞。</p> <p>3. 建置 VANS 弱點修補系統，整合端點防護軟體資訊蒐集，採自動化方式與中控台強制報到修補，降低零時差惡意探索被攻擊之風險。</p> <p>4. 透過串接 API 整合弱點修補數據，建立視覺化儀表板，呈現端點設備、伺服器主機、系統網站弱點修補情形。</p>
--	--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

十、相關聯絡資料

縣(市)政府	機關名稱	聯絡人姓名	電話	E-mail
臺南市政府	智慧發展中心	邱文志	06-2991111#8060	itel41@mail.tainan.gov.tw
臺南市政府	智慧發展中心	洪將涵	06-2991111#8741	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