政府科技發展中程個案計畫書

科技發展類前瞻基礎建設計畫

審議編號：112-3601-09-20-01

數位發展部資通安全署

（數位發展部資通安全署）

「政府基層機關資安主動防禦計畫（1 / 2)」

（核定本）

計畫全程：112 年 01 月至 113 年 12 月

中華民國 111 年 09 月

政府科技發展計畫書修正對照表(A009)

審議編號：112-3601-09-20-01

計畫名稱：政府基層機關資安主動防禦計畫

申請機關(單位)：數位發展部資通安全署

序號	審查意見	計畫修正說明	修正處頁碼
1	計畫延續前瞻基礎建設計畫第一期強化政府基層機關資安防護及區域聯防計畫，協助地方政府持續強化資安防護，精進產學合作，符合國家資通安全發展方案(110 年至 113 年)中「賡續推動政府資訊(安)集中共享」之措施。	感謝委員支持。	
2	推動地方政府資訊資源向上集中，可有效提升地方政府資訊資源及資安(訊)人力運用效率，減少資源重複投資；導入 VANS 有助於提升地方政府茲安防護能量；考量國際資安威脅日益嚴峻，而地方政府相關系統有其弱點，為協助地方政府資安防護永續經	感謝委員支持。	

序號	審查意見	計畫修正說明	修正處頁碼
	營，本計畫推動有其必要性及迫切性。		
3	目標及關鍵成果部分 (1)本計畫預計在本期將所有地方政府導入VANS，並讓所有B級地方政府機關導入EDR，關鍵成果與目標明確。 (2)促進產官學合作部分，推動資安業界與在地政府與學界合作驗證，有助協助找出可能資安威脅。地方政府結合國內大專院校合作培訓資安人才對我國資安人才培育也有助益，但是其成果產出應該更明確要求，並強化計畫之各年度期中查證。 (3)本計畫所擬定之關鍵成果與目標扣合度高，惟成果大多以操作型指標展現，不易	感謝委員支持。	

序號	審查意見	計畫修正說明	修正處頁碼
	評估其執行品質。建議本計畫預期關鍵成果中增加地方政府之執行效益(或續用前期相關執行之主要績效指標)，以利展現推動成果與亮點。 (4) 計畫目前已修正可檢核之最終效益，應搭配對各地方政府計畫成果之落實查核。 (5) 本計畫 112 年度與 113 年度之目標與預期關鍵成果大多相似或相同，建議依全程執行進度設計不同年度之目標，以展現本計畫推動之進階性及進展。		
4	執行面建議 (1) 本計畫促進產官學合作部分宜與國科會學術型資安研究計畫搭配，共同串接學校研究與人才資源。 (2) 本計畫主要目標之一為「精進資安防護能	感謝委員支持。	

序號	審查意見	計畫修正說明	修正處頁碼
	量」，惟各地方政府所轄之資安防護能力(技術與人力)不一，各分項/縣市計畫書中所述之作法也不相同；本計畫推動時提案單位宜加強督導或進行期中查證，並協助防護力較弱或執行力較弱的縣市完善其推動策略。 (3)減少網路攻擊介面及增加資訊流能見度是資安基礎建設，本計畫規劃之資料中心向上集中策略，可減少各地方政府在資安管理上的能量欠缺問題，藉由單一資料中心，能有效減少攻擊介面，同時將有限資源聚焦在單一資料中心的防護上，應該在政府資安基礎建設強化中落實。 (4)弱點管理與修補，資安態勢的掌控也是近年來國際資安防禦的		

序號	審查意見	計畫修正說明	修正處頁碼
	重要策略，透過VANS機制的佈建，對於C級機關的弱點管控確有其必要性，而B級機關EDR的佈建，對於資源欠缺的地方政府，是當務之急。計畫執行單位亦針對各地方政府財務能力，訂定不同補助比例，有助於政府資源的有效運用。但須追蹤運用成效。		
5	計畫預期效益部分 (1)本計畫預期效益，集中建置整體資安防護，以有效人力、資源共用目標明確，但目前地方政府資料中心約350個以上，每年集中10個資料中心效益不大，應予提高至少減少40個以上(淨值)。 (2)推動地方政府產官學合作及實證場域部分對於提升地方政府資	(1)推動地方政府資源向上集中，為提升資訊資源及資安人力運用效率，各機關資訊系統採縣市政府統籌維運、資安控管集中需要，惟部分機關涉全國性業務及資通系統，有個別集中需求，如地政、稅務、警政、消防等，配合實務議題，爰本計畫預計112年以逐年縮減10個資料中心為目標，並以15個為	(1)2、5、6、7、8、13、22、25 (2)2、5、7、14、23

序號	審查意見	計畫修正說明	修正處頁碼
	安防護效益不明確，且每年培訓人才 30 人次過少，應改為人數，並請資安處補充所培育的人才的資安職能。 (3) 本計畫承接前期計畫成果，切合「資安即國安」政策方針，透過整體資安聯合防禦機制，以有效防範政府機關遭受資安攻擊之風險，規劃完整可行，切合需求。本計畫所擬定之自我挑戰目標適切可行。	挑戰目標，並依委員意見將指標修正為「計畫執行機關完成所屬機關資料中心減量，降低線路分散程度」。 (2) 本計畫推動由地方政府搭配國內大專院校、業界培育資安策略面、管理面、技術面之資安職能，各縣市政府依其資安作業需求，培訓數位鑑識或網路攻防人才，有關培訓量能將依委員建議調整為人數，提升為 50 人(修正計畫第 2、5、7、14、23 頁)，後續視推動情形滾動檢討。	
6	本計畫經費考量地方政府需求，以及作為院資安處轉入數位部的過渡時期作法，建議支持，但申請單位需配合以下事項： (1) 院資安處未來轉入數	感謝委員支持，本案計畫啟動時間為 112 年，屆時將與數位發展部併同考量相關做法，使補助作業有所依循。	

序號	審查意見	計畫修正說明	修正處頁碼
	位部，將無法沿用行政院補助地方政府強化資通安全防護作業要點補助地方政府，需另訂要點。 (2)不符合本計畫工作項目的地方政府提案不在補助之列，應優先刪減。		
7	本案計畫雖已修正最終效益及各年度目標，惟仍未能有效呈現防禦能力提升，僅屬於投入面指標訂定，後續仍請精進調整，並補充網路及應用韌性提升指標訂定。	指標修正為「計畫執行機關完成所屬機關資料中心減量，降低線路分散程度」，112 年指標達 5%，113 年指標達 10%，以提升網路及應用韌性。	2、5、6、7、8、13、22、25
8	請提出本案計畫後續維運之規劃說明，尤其針對未提出經費需求之地方政府。	(1)金門縣政府規劃於 112 年建置系統，後續以保固方式維運，113 年由該府自行編列經費辦理維護及營運。 (2)嘉義市政府規劃於 112 年建置系統，於 113 年將 EDR 相關成果分析以利調整改	

序號	審查意見	計畫修正說明	修正處頁碼
		善，後續以軟體升級授權(MA)方式維運。	
9	本案計畫刪除產官學合作部分，轉為其他績效指標進行運作，包括加強滲透測試及紅藍軍攻防演練內容規劃。	本案計畫刪除產官學於實證場域合作部分，轉為擴大於滲透測試、紅藍軍攻防演練內容等強化資安規劃，引入資安人才之產學交流。	1、2、3、5、7、8、11、12、13、15、19、22、25
10	本案計畫請執行單位於文到一週內提出執行模式、工作項目及 KPI 修正內容，由科技會報辦公室會同審查委員檢視確認，並視需求另案召開專案會議。	調整政府基層機關資安主動防禦計畫執行模式、工作項目及KPI。	2、5、6、7、8、13、14、22、23、25、26、27
11	本計畫 112 年與 113 年建議經費核定數為每年 4.6 億元。	依核定數調整計畫及各項子計畫核定經費。	4、5、21、22、25、58、附件 1-6
12	本案係開放地方政府申請經費之補助型計畫，有關本計畫補助執行機關辦理培育資安人才活動部分，為改善長期以	請各地方政府於計畫內加入鼓勵弱勢性別參與措施，並於報送相關活動成果時納入性別統計資料。	15

序號	審查意見	計畫修正說明	修正處頁碼
	來資通訊領域人才性別落差，建議將「鼓勵弱勢性別參與措施」納入審查各執行機關提送計畫之要項，以降低科技領域人才之性別區隔；並請執行機關報送相關活動成果時，納入性別參與之統計資料，以瞭解其推動前揭衡平性別比例措施之成效，俾作為未來辦理相關培育資安人才活動之參考。		
13		為行政院資通安全處組改為數位發展部資通安全署，修正相關機關名稱。(因內文已奉院核定，不做修正)	1、2、4、5、6、封面、修正對照表
14		為行政院資通安全處組改為數位發展部資通安全署，關聯施政目標調整為數位發展部研提項目：07:提升國家數位發展環境之資安防護韌性。	1、2

附表、計畫目標及預期關鍵成果之修正對照表(修正核定版填寫)

項目	送審版	核定版	
經費	送審數 112 年：500,000 千元 113 年：500,000 千元	核定數 112 年：460,000 千元 113 年：460,000 千元	修正說明
計畫目標及預期關鍵成果	目標 1：推動地方政府資訊資源向上集中。 關鍵成果 1:計畫執行機關完成所屬機關資料中心減量，計 10 個資料中心向上集中至計畫執行機關。	目標 1: 推動地方政府資訊資源向上集中。 關鍵成果 1: 計畫執行機關完成所屬機關資料中心減量，降低線路分散程度達 5%。	為有效呈現防禦能力提升，依委員意見將指標修正為「計畫執行機關完成所屬機關資料中心減量，降低線路分散程度」，112 年指標達 5%，113 年指標達 10%，以提升網路及應用韌性。
	目標 2：精進地方政府資安防護能量。 關鍵成果 1:符合資通安全責任等級 C 級之地方政府均導入資訊系統弱點通報機制(VANS)。 關鍵成果 2:符合資通安全責任等級 B 級之地方政府均導入端點偵測及應變機制(EDR)。	目標 2: 精進地方政府資安防護能量。 關鍵成果 1: 符合資通安全責任等級 C 級之地方政府均導入資訊系統弱點通報機制(VANS)。 關鍵成果 2: 符合資通安全責任等級 B 級之地方政府均導入端點偵測及應變機制(EDR)。 關鍵成果 3: 導入 VANS 之地方政府機關設備所發現 CVSS 7 分以上資安弱點於 1 週內完成處置達 70%。	為有效呈現防禦能力提升，依委員意見將指標修正為「導入 VANS 之地方政府機關設備所發現 CVSS 7 分以上資安弱點於 1 週內完成處置比例」，112 年指標達 70%，113 年指標達 75%，以提升地方政府資

			安防護能量。
	目標 3：推動地方政府產官學合作及實證場域。 關鍵成果 1:與國內大專院校合作，培訓人才至少 30 人次。 關鍵成果 2:推動紅藍隊演練或資安檢測至少 6 案，協助地方政府改善資安防護。	目標 3: 推動滲透測試及紅藍軍攻防演練。 關鍵成果 1: 與國內大專院校合作，培訓人才至少 50 人。 關鍵成果 2: 推動紅藍隊演練或資安檢測至少 6 案，協助地方政府改善資安防護。	本計畫推動由地方政府搭配國內大專院校、業界培育資安策略面、管理面、技術面之資安職能，各縣市政府依其資安作業需求，培訓數位鑑識或網路攻防人才，有關培訓量能將依委員建議調整為人數，提升為 50 人，後續視推動情形滾動檢討。

■請機關檢核確認業依審議通過之預算數及各項審查意見，妥適完成計畫內容修正(含計畫目標及預期關鍵成果修正)　■是 □否

目 錄

壹、基本資料及概述表(A003)

<table>
<tr><td>審議編號</td><td colspan="4">112-3601-09-20-01</td></tr>
<tr><td>計畫名稱</td><td colspan="4">政府基層機關資安主動防禦計畫</td></tr>
<tr><td>申請機關</td><td colspan="4">數位發展部資通安全署</td></tr>
<tr><td>預定執行機關
(單位或機構)</td><td colspan="4">數位發展部資通安全署、臺北市(花蓮縣、連江縣、金門縣)、新北市(基隆縣、宜蘭縣)、桃園市(新竹市、新竹縣、苗栗縣)、臺中市(彰化縣、南投縣)、臺南市(嘉義市、嘉義縣、雲林縣)、高雄市(屏東縣、澎湖縣、臺東縣)</td></tr>
<tr><td rowspan="3">預定
計畫主持人</td><td>姓名</td><td>謝翠娟</td><td>職稱</td><td>署長</td></tr>
<tr><td>服務機關</td><td colspan="3">數位發展部資通安全署</td></tr>
<tr><td>電話</td><td>○○○</td><td>電子郵件</td><td>○○○</td></tr>
<tr><td>計畫摘要</td><td colspan="4">資通安全管理法(以下簡稱資安法)於 108 年施行至今逾 3 年，為協助地方政府落實法遵事項，並考量各地方政府經費、人力及資安防護技術能量不同，106-109 年透過前瞻計畫，透由建構地方政府區域聯防體系，以 6 個直轄市為核心，結合周邊鄰近縣市推動區域聯防架構，建立事前監控(SOC)、事中通報(CERT)，與事後分享(ISAC)等機制，進行相關資安監控、即時應處及情資分享，整體提升區域內的資安防護；並於 110 年透過跨部會署科技計畫協助地方政府導入資安弱點通報機制(VANS)及推動向上集中。考量國際資安威脅日益嚴峻，為協助地方政府資安防護永續經營，爰計畫規劃方向如下：
一、推動地方政府資訊資源向上集中：透過資訊資源向上集中，提升地方政府資訊資源及資安(訊)人力運用效率，減少資源重複投資。
二、精進地方政府資安防護能量：配合資訊資源向上集中之必要資安防護需求，並推動導入資訊系統弱點通報機制(VANS)、端點偵測及應變機制(EDR)等資通安全管理法所訂應辦事項。
三、滲透測試及紅藍軍攻防演練：推動進行擴大資安防護之滲透測試及紅藍軍攻防演練，強化地方政府資安基礎環境並培育資安人才，達成資安人才之產學交流。</td></tr>
<tr><td rowspan="3">計畫目標、預期關鍵成果及與部會科技施政目標之關聯</td><td colspan="2">計畫目標及預期關鍵成果</td><td rowspan="2">與部會科技施政目標之關聯</td></tr>
<tr><td>112 年度</td><td>113 年度</td></tr>
<tr><td>目標 1: 推動地方政府資訊資源向上集中。</td><td>目標 1: 推動地方政府資訊資源向上集中。</td><td>數位發展部:07: 提升國家數位發展環境之資安防護韌性</td></tr>
</table>

	關鍵成果 1：計畫執行機關完成所屬機關資料中心減量，降低線路分散程度達 5%。	關鍵成果 1：計畫執行機關完成所屬機關資料中心減量，降低線路分散程度達 10%。	
	目標 2：精進地方政府資安防護能量。 關鍵成果 1：符合資通安全責任等級 C 級之地方政府均導入資訊系統弱點通報機制(VANS)。 關鍵成果 2：符合資通安全責任等級 B 級之地方政府均導入端點偵測及應變機制(EDR)。 關鍵成果 3：導入 VANS 之地方政府機關設備所發現 CVSS 7 分以上資安弱點於 1 週內完成處置達 70%。	目標 2：精進地方政府資安防護能量。 關鍵成果 1：符合資通安全責任等級 B 級之地方政府依資通安全管理法主管機關指定之方式提交端點偵測及應變機制(EDR)偵測資料。 關鍵成果 2：導入 VANS 之地方政府機關設備所發現 CVSS 7 分以上資安弱點於 1 週內完成處置達 75%。	數位發展部:07：提升國家數位發展環境之資安防護韌性
	目標 3：推動滲透測試及紅藍軍攻防演練。 關鍵成果 1：與國內大專院校合作，培訓人才至少 50 人。 關鍵成果 2：推動紅藍隊演練或資安檢測至少 6 案，協助地方政府改善資安防護。	目標 3：滲透測試及紅藍軍攻防演練。 關鍵成果 1：與國內大專院校合作，培訓人才至少 50 人。 關鍵成果 2：推動紅藍隊演練或資安檢測至少 6 案，協助地方政府改善資安防護。	數位發展部:07：提升國家數位發展環境之資安防護韌性
預期效益	依國家安全會議於 107 年 9 月訂頒「國家資通安全戰略報告：資安即國安」政策方針，為強化國家整體資通安全之防禦能量，爰透過中央機關與地方政府整體資安聯合防禦機制，以有效防範政府機關遭受資安攻擊之風險，本計畫係延續區域聯防的架構概念，協助地方政府持續強化資安防護，精進產學合作，研析資安技術，預期效益重點說明如下：		

<table>
<tr><td></td><td colspan="2">1. 推動地方政府資訊資源向上集中：朝單一資料中心為目標，縮減現有資料中心數量，建置共用資料中心，發展共用系統，並搭配整併線路集中網路出口，縮減資安防護缺口。
2. 精進地方政府資安防護能量：導入 VANS 將資通訊設備盤點之資產資訊彙整上傳至 VANS 系統，當有新的資安弱點發布時，透由系統主動即時比對通知，取代以往人工方式逐一調查受影響之資通訊設備數量，即時準確掌握受影響的設備數量，快速制定防護策略，依優先順序進行弱點修補，進行風險控管，有效提升整體效率。藉由導入 EDR，針對端點設備持續偵測異常行為或惡意程式活動，進行分析提供人員早期預警處置，避免資安事件的發生，並透過現有的聯防監控管道提供監控資訊，後續可作為聯防監控的參考，轉為相應情資進行聯合防禦，達成法遵要求事項。
3. 滲透測試及紅藍軍攻防演練：推動進行擴大資安防護之滲透測試及紅藍軍攻防演練，強化地方政府資安基礎環境並培育資安人才，達成資安人才之產學交流。</td></tr>
<tr><td>計畫群組
及比重</td><td colspan="2">請依群組比重填寫，需有比重最高之群組，且加總須 100%。
□ 生命科技 ____ %　□環境科技 ____ %　■數位科技 100 %
□ 工程科技 ____ %　□人文社會 ____ %　□科技創新 _____ %</td></tr>
<tr><td>計畫類別</td><td colspan="2">■ 前瞻基礎建設計畫</td></tr>
<tr><td>前瞻項目</td><td colspan="2">□ 綠能建設　■ 數位建設　□ 人才培育促進就業之建設</td></tr>
<tr><td>推動 5G 發展</td><td colspan="2">□ 是　■ 否</td></tr>
<tr><td>資通訊建設計畫</td><td colspan="2">■ 是　□ 否</td></tr>
<tr><td>政策依據</td><td colspan="2">1. FIDP-20210201020000：前瞻基礎建設計畫：1.2 強化政府基層機關資安防護及區域聯防
2. NICSP-20210301000000：國家資通安全發展方案(110年至113 年)：1. 賡續推動政府資訊(安)集中共享</td></tr>
<tr><td>計畫額度</td><td colspan="2">■ 前瞻基礎建設額度</td></tr>
<tr><td>執行期間</td><td colspan="2">112 年 01 月 01 日　至 112 年 12 月 31 日</td></tr>
<tr><td>全程期間</td><td colspan="2">112 年 01 月 01 日　至 113 年 12 月 31 日</td></tr>
<tr><td rowspan="2">前一年度預算</td><td>年度</td><td>經費(千元)</td></tr>
<tr><td>111</td><td>0</td></tr>
</table>

<table>
<tr><td rowspan="15">資源投入</td><td>年度</td><td colspan="4">經費(千元)</td></tr>
<tr><td>110</td><td colspan="4">0</td></tr>
<tr><td>111</td><td colspan="4">0</td></tr>
<tr><td>112</td><td colspan="4">460,000</td></tr>
<tr><td>113</td><td colspan="4">460,000</td></tr>
<tr><td>114</td><td colspan="4">0</td></tr>
<tr><td>合計</td><td colspan="4">920,000</td></tr>
<tr><td rowspan="5">112 年度</td><td>人事費</td><td>0</td><td>土地建築</td><td>0</td></tr>
<tr><td>材料費</td><td>0</td><td>儀器設備</td><td>0</td></tr>
<tr><td>其他經常支出</td><td>233,182.530</td><td>其他資本支出</td><td>226,817.470</td></tr>
<tr><td>經常門小計</td><td>233,183.530</td><td>資本門小計</td><td>226,817.470</td></tr>
<tr><td colspan="2">經費小計(千元)</td><td colspan="2">460,000</td></tr>
<tr><td rowspan="5">113 年度</td><td>人事費</td><td>0</td><td>土地建築</td><td>0</td></tr>
<tr><td>材料費</td><td>0</td><td>儀器設備</td><td>0</td></tr>
<tr><td>其他經常支出</td><td>232,135.850</td><td>其他資本支出</td><td>227,864.150</td></tr>
<tr><td>經常門小計</td><td>232,135.850</td><td>資本門小計</td><td>227,864.150</td></tr>
<tr><td colspan="2">經費小計(千元)</td><td colspan="2">460,000</td></tr>
<tr><td>部會施政計畫關鍵策略目標</td><td colspan="5">自系統選取主管機關之部會施政計畫關鍵策略目標。</td></tr>
<tr><td>本計畫在機關施政項目之定位及功能</td><td colspan="5">一、我國資通安全管理法於108年1月1日施行，目的為積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益。數位發展部資通安全署作為國家資通安全會報之幕僚單位，持續推動資安政策並推動發展建構強韌的資安生態。
二、依國家安全會議於107年9月訂頒「國家資通安全戰略報告：資安即國安」政策方針，為強化國家整體資通安全之防禦能量，推動中央機關與地方政府整體資安聯合防禦機制，降低資安破口，以有效防範政府機關遭受資安攻擊之風險，以期建立可信賴的資通安全環境，保障民眾權</td></tr>
</table>

<table>
<tr><td></td><td colspan="6">益。
三、本計畫協助地方政府持續精進資安防護能量，並依「國家資通安全發展方案(110年至113年)」之推動策略：「善用智慧前瞻科技，主動抵禦潛在威脅」，藉由發展之人工智慧工具分析大量之資安數據情資，提前掌握資安事件攻擊前兆，先行預防應對，並由數位發展部資通安全署依據上述政策方針，透過導入 VANS、EDR 強化資安防護，產學協力、實證資安防護成效及研析資安技術，降低政策導入風險。</td></tr>
<tr><td rowspan="5">計畫架構說明</td><td colspan="6">依細部計畫說明</td></tr>
<tr><td>細部計畫
名稱</td><td colspan="5">政府基層機關資安主動防禦計畫</td></tr>
<tr><td>112 年度
概估經費(千元)</td><td>460,000</td><td rowspan="2">計畫性質</td><td rowspan="2">請以下拉選單選擇此細部計畫之計畫性質</td><td rowspan="2">預定執行機構</td><td rowspan="2">數位發展部資通安全署</td></tr>
<tr><td>113 年度
概估經費(千元)</td><td>460,000</td></tr>
<tr><td>細部計畫
重點描述</td><td colspan="5">一、推動地方政府資訊資源向上集中：透過資訊資源向上集中，提升地方政府資訊資源及資安(訊)人力運用效率，減少資源重複投資。
二、精進地方政府資安防護能量：配合資訊資源向上集中之必要資安防護需求，並推動導入資訊系統弱點通報機制(VANS)、端點偵測及應變機制(EDR)等資通安全管理法所訂應辦事項。
三、滲透測試及紅藍軍攻防演練：推動進行擴大資安防護之滲透測試及紅藍軍攻防演練，強化地方政府資安基礎環境並培育資安人才，達成資安人才之產學交流。</td></tr>
<tr><td>主要績效指標 KPI
(請填寫此細部計畫之主要績效指標(至多 3 項))</td><td colspan="5">112 年主要績效指標：
1-1 計畫執行機關完成所屬機關資料中心減量，降低線路分散程度達 5%。
2-1 符合資通安全責任等級 C 級之地方政府均導入資訊系統弱點通報機制(VANS)。
2-2 符合資通安全責任等級 B 級之地方政府均導入端點偵測及應變機制(EDR)。
2-3 導入 VANS 之地方政府機關設備所發現 CVSS 7 分以上資安弱點於 1 週內完成處置達 70%。</td></tr>
</table>

<table>
<tr><td></td><td></td><td>3-1 與國內大專院校合作，培訓人才至少 50 人。
3-2 推動紅藍隊演練或資安檢測至少 6 案，協助地方政府改善資安防護。</td></tr>
<tr><td></td><td></td><td>113 年主要績效指標：
1-1 計畫執行機關完成所屬機關資料中心減量，降低線路分散程度達 10%。
2-1 符合資通安全責任等級 B 級之地方政府依資通安全管理法主管機關指定之方式提交端點偵測及應變機制(EDR)偵測資料。
2-2 導入 VANS 之地方政府機關設備所發現 CVSS 7 分以上資安弱點於 1 週內完成處置達 75%。
3-1 與國內大專院校合作，培訓人才累計至少 100 人。
3-2 推動紅藍隊演練或資安檢測累計至少 12 案，協助地方政府改善資安防護。</td></tr>
<tr><td>前一年計畫或相關之前期程計畫名稱</td><td colspan="2">1. 前瞻基礎建設-數位建設「強化政府基層機關資安防護及區域聯防計畫」(106-109年)
2. 跨部會署科技計畫-強化政府基層機關資安防護計畫(110年7月-111年6月)</td></tr>
<tr><td>前期
主要績效</td><td colspan="2">1. 已完成建置資安監控機制二線 SOC。
2. 區域聯防涵蓋範圍達 81.62%。
3. 導入政府組基準比例(A、B 級)100%。
4. 個人電腦國產品採購比例 100%。
5. 其他國產品採購比例 62.99%。
6. 地方政府資通安全責任等級 B 級以上機關導入介接 VANS 機制達 100%。</td></tr>
<tr><td>中英文關鍵詞</td><td colspan="2">地方政府、國家資通安全發展方案、資安弱點通報機制、端點偵測及應變機制、資通安全
Local Government, National Cyber Security Program, Vulnerability Alert and Notification System, Endpoint Detection and Response, Cyber Security</td></tr>
<tr><td rowspan="3">計畫連絡人</td><td>姓名</td><td>史凱文</td><td>職稱</td><td>分析師</td></tr>
<tr><td>服務機關</td><td colspan="3">數位發展部資通安全署</td></tr>
<tr><td>電話</td><td>○○○</td><td>電子郵件</td><td>○○○</td></tr>
</table>

附錄 - 最終效益與各年度里程碑規劃表

最終效益(Endpoint)與里程碑(Milestone)規劃	修正說明
最終效益： 達成機關資料中心減量，降低線路分散程度達，導入 VANS 及 EDR 以精進地方政府資安防護能量，並培育在地資安人才	
112 年度里程碑： 【年度目標】 1.推動地方政府資訊資源向上集中。 2.精進地方政府資安防護能量。 3.推動滲透測試及紅藍軍攻防演練。 【關鍵成果】 1-1 計畫執行機關完成所屬機關資料中心減量，降低線路分散程度達 5%。 2-1 符合資通安全責任等級 C 級之地方政府 100%導入資訊系統弱點通報機制(VANS)。 2-2 符合資通安全責任等級 B 級之地方政府 100%導入端點偵測及應變機制(EDR)。 2-3 導入 VANS 之地方政府機關設備所發現 CVSS 7 分以上資安弱點於 1 週內完成處置達 70%。 3-1 與國內大專院校合作，培訓人才至少 50 人。 3-2 推動紅藍隊演練或資安檢測至少 6 案，協助地方政府改善資安防護。	

最終效益(Endpoint)與里程碑(Milestone)規劃	修正說明
113 年度里程碑： 【年度目標】 1. 推動地方政府資訊資源向上集中。 2. 精進地方政府資安防護能量。 3. 推動滲透測試及紅藍軍攻防演練。 【關鍵成果】 1-1 計畫執行機關完成所屬機關資料中心減量，降低線路分散程度達 10%。 2-1 新增符合資通安全責任等級 B 級之地方政府依資通安全管理法主管機關指定之方式提交端點偵測及應變機制(EDR)偵測資料 2-2 導入 VANS 之地方政府機關設備所發現 CVSS 7 分以上資安弱點於 1 週內完成處置達 75%。 3-1 與國內大專院校合作，培訓人才累計至少 100 人。 3-2 推動紅藍隊演練或資安檢測至少 6 案，協助地方政府改善資安防護。	

貳、計畫緣起

一、政策依據

隨著全球數位科技蓬勃發展，新興資訊科技及駭客攻擊手法亦日趨多元，致資安威脅日趨嚴峻，因此持續落實精進各項資安防護工作，實屬必要。依國家安全會議於107年9月訂頒「國家資通安全戰略報告：資安即國安」政策方針，強化國家整體資通安全之防禦能量，爰透過中央機關與地方政府整體資安聯合防禦機制，以有效防範政府機關遭受資安攻擊之風險。

本計畫為提升地方政府資安防護能量，並依「國家資通安全發展方案(110年至113年)」之推動策略：「善用智慧前瞻科技，主動抵禦潛在威脅」，藉由發展人工智慧工具分析大量數據情資，提前掌握資安事件攻擊前兆，並先行預防應對。為達此目標，期將地方政府資訊資源向上集中，透過整併各地方政府所屬機關之資料中心，集中資安防護能量，另為提升端點資安防護，配合法遵事項推動地方政府及其所屬機關導入VANS、EDR，提升整體資安防護能量。

二、擬解決問題之釐清

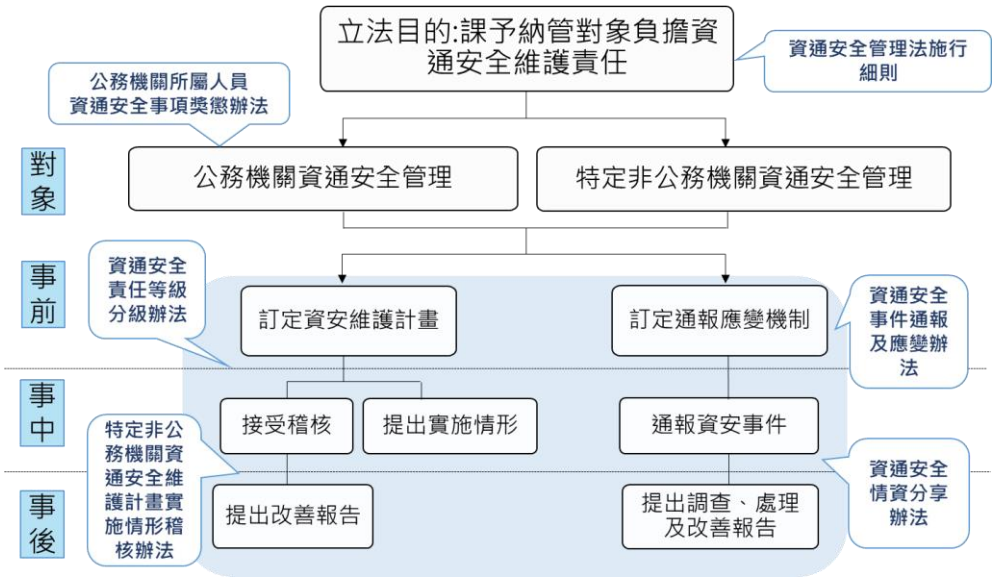
鑒於國際資安威脅情勢日趨嚴峻，如何完善政府機關資安防護，使我國面對全球資安高風險，仍能穩健發展為首重目標，為建構完善的國家資通安全環境，我國於108年施行資通安全管理法，另訂定六項子法同步施行，明定落實各項資安作業，惟地方政府時常反應資安人力及經費普遍不足，致業務繁重且推動資安防護有限，為解決上述問題，本計畫推動地方政府資源服務向上集中，協助將資通訊資源及人力向上集中，有效運用有限資源避免過度分散，並透由自動化系統及標準化程序減少人力負擔，其中導入介接VANS，係將資通訊設備盤點之資產資訊彙整上傳至VANS系統，於新的資安弱點發布時，透由系統主動即時比對通知，取代人工逐一調查受影響之資通訊設備數量，快速制定防護策略，並推動導入EDR，以持續偵測端點異常行為或惡意活動，主動發現端點的潛在威脅，從而降低可能的資安風險，加強資安實戰人才培育，落實資安產業人才在地深根，降低資安人才的缺口。

三、目前環境需求分析與未來環境預測說明

為強化國家資通安全環境，各先進國家皆透過研訂相關資通安全法規與標準，作為完備資安基礎環境的關鍵環節。我國經過多方說明座談、溝通及協調，於107年6月6日總統令公布「資通安全管理法」，為

我國首部資安專法，並於108年1月1日起正式施行，明定落實各項資安作業，依資通安全管理法制定的六項子法亦同步施行。透過資通安全管理法施實，將資安作業應配置之資源及辦理事項納為法遵事項，提升機關瞭解及認知資安工作，並於110年滾動式調修資通安全管理法相關子法，訂定機關應完成的應辦事項，以因應目前的資安環境需求，打造可信賴的資通訊服務。

我國資通安全管理法及六項子法架構



另有關未來資通安全發展規劃方向，依據聯合國之國際電信聯盟(ITU)於2018年發布之全球資通安全指標，並對美洲區、歐洲區、亞太區等區域國家做資安綜合考量排名，排名較高之國家有美國、加拿大、英國、日本、韓國等，前述各國近兩年提出之國家資通安全戰略，可歸納為「建立主動式防禦之資安聯防體系」、「提高網路攻擊應變能力」、「深化公私協同治理以提升民間防護能量」等方向發展，並考量新興科技發展和IoT設備普及，以及5G時代來臨，資通威脅日益加劇，爰110年推動國家資通安全發展方案(110年至113年)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。

本計畫係依據「國家資通安全發展方案(110年至113年)」之推動策略三「善用智慧前瞻科技，主動抵禦潛在威脅」，協助各地方政府善用智慧前瞻科技主動抵禦潛在威脅，推動資訊資源向上集中策略，賡續落實資安防護工作，整體提升國家防護水準。

四、本計畫對社會經濟、產業技術、生活品質、環境永續、學術研究、人才培育等之影響說明

（一）產業技術：本計畫統合地方政府資安需求，以資訊資源向上集中為策略，進行共用資料中心及共用性系統規劃，提昇資源運用效率，輔以業界新興資安防護技術，提升整體資安量能。

（二）人才培育：推動滲透測試及紅藍軍攻防演練，進行擴大資安防護之滲透測試及紅藍軍攻防演練，強化地方政府資安基礎環境並培育資安人才，達成資安人才之產學交流。

參、計畫目標與執行方法

一、目標說明

我國現正推動「數位國家・創新經濟發展方案」及「5+2 產業創新計畫」，皆為強化我國智能數位發展以及驅動下世代產業創新，為經濟成長注入新動能。而茁壯發展數位科技，首先須具備安全之數位環境為基底，因此資通訊安全防護將為關鍵。

本計畫於第一階段(106-109 年)已完成建構區域聯防機制，並且為解決資通訊終端設備安全性設定不一及人員管理不易之問題，導入戶役、地政、稅政、衛政、社政及基層公所工作站之政府組態基準(GCB)，同時汰換 7 年以上或無法進行安全性更新之工作站，降低資訊作業之潛在風險，協助地方政府建立防護基礎。為進一步強化地方政府資安防護，持續推動資訊資源向上集中，提升地方政府資訊資源及資安(訊)人力運用效率，減少資源重複投資。

配合資訊資源向上集中，資料中心及核心資通系統應有更積極防護策略，如資源集中整併網路線路單一出口，精進各項資安防護，以及推動導入介接 VANS，透過資產弱點比對掌握機關內具有漏洞或弱點之資通設備範圍，進一步執行安全性更新或防護，以降低遭受攻擊風險，及導入 EDR，針對端點設備持續偵測異常行為或惡意程式活動，進行分析提供人員早期預警處置。另一方面可開放政府場域，與大專校院合作，提供學生進行資安研究成果實證，將所學理論轉化實際應用，亦可搭配與資安產業進行滲透測試與攻防演練，針對向上集中所需搭配之資安防護機制進行解決方案之技術交流，共同提昇整體資安防護能量。

（一）本計畫全程預期目標：

1. 資訊資源向上集中：透過資訊資源向上集中，提升地方政府資訊資源及資安(訊)人力運用效率，減少資源重複投資。
2. 精進資安防護能量：因應資訊資源向上集中，提升集中所需資安防護之軟體、硬體及服務能量，及推動導入 VANS 及 EDR。
3. 滲透測試及紅藍軍攻防演練：推動進行擴大資安防護之滲透測試及紅藍軍攻防演練，強化地方政府資安基礎環境並培育資安人才，達成資安人才之產學交流。

（二）各項目標預期工作項目：

1. 資訊資源向上集中：建置共用資料中心、建置及推廣共用性系統。依據「行政院及所屬各機關資料中心設置作業要點」，

資料中心係指各機關為供資通訊系統正常運行所設置之基礎及備援設施，其主要設施包含運算伺服主機、儲存設備、網通設備、資安設備、環境控制設施及存放前述設施之實體空間。

2. 精進資安防護能量：配合資訊資源向上集中之必要資安防護需求、推 VANS、EDR。
3. 滲透測試及紅藍軍攻防演練：推動進行擴大資安防護之滲透測試及紅藍軍攻防演練，強化地方政府資安基礎環境並培育資安人才，達成資安人才之產學交流。

（三）計畫全程總目標、年度目標及預期關鍵成果：

計畫全程總目標(end point)					
推動地方政府資訊資源向上集中 精進地方政府資安防護能量 推動滲透測試及紅藍軍攻防演練					
里程碑(milestone)					
年度	第一年 民 110 年	第二年 民 111 年	第三年 民 112 年	第四年 民 113 年	第四年 民 114 年 (8 月)
年度目標	計畫未開始	計畫未開始	1. 地方政府資料中心減量，朝單一資料中心為目標。 2. 地方政府配合法遵要求事項，精進資安防護能量。 3. 推動滲透測試及紅藍軍攻防演練	1. 地方政府資料中心減量，朝單一資料中心為目標。 2. 地方政府配合法遵要求事項，精進資安防護能量。 3. 推動滲透測試及紅藍軍攻防演練	無
預期關鍵成果	計畫未開始	計畫未開始	1-1 計畫執行機關完成所屬機關資料中心減量，降低線路分散程度達 5%。 2-1 符合資通安全責任	1-1 計畫執行機關完成所屬機關資料中心減量，降低線路分散程度達 10%。 2-1 符合資通安全責任	無

			等級C級之地方政府均導入資訊系統弱點通報機制(VANS)。 2-2 符合資通安全責任等級B級之地方政府均導入端點偵測及應變機制(EDR)。 2-3 導入VANS之地方政府機關設備所發現CVSS 7分以上資安弱點於1週內完成處置達70%。 3-1 與國內大專院校合作，培訓人才至少50人。 3-2 推動紅藍隊演練或資安檢測至少6案,協助地方政府改善資安防護。	等級B級之地方政府依資通安全管理法主管機關指定之方式提交端點偵測及應變機制(EDR)偵測資料。 2-2 導入VANS之地方政府機關設備所發現CVSS 7分以上資安弱點於1週內完成處置達75%。 3-1 與國內大專院校合作，培訓人才至少50人。 3-2 推動紅藍隊演練或資安檢測至少6案,協助地方政府改善資安防護。	
年度目標達成情形(重大效益)	計畫未開始	計畫未開始			

二、執行策略及方法

本計畫延續區域聯防之推動概念，加強區域合作，以6個直轄市為核心，涵蓋鄰近區域，規劃由直轄市彙整區域縣市需求進行計畫提報，

內容應扣合本計畫之全程總目標，並就資訊資源向上集中、精進資安防護能量及推動資安實戰人才培育進行全面評估及整體規劃，同時提出計畫補助結束後之永續經營模式。由本院資通安全處透過計畫審查機制，審查具備合理性及完整性之地方政府提案內容，補助該地方政府推動執行，並依「行政院補助地方政府強化資通安全防護作業要點」定期進行管考，確保計畫如期、如質順利完成。

本計畫屬競爭型計畫，地方政府提報之計畫內容應扣合本計畫之全程總目標，並就資訊資源向上集中、精進資安防護能量、推動資安實戰人才培育等項目進行全面評估及整體規劃，並提前規劃計畫補助結束後之永續經營模式；本處並透過 VANS 後台系統每月檢視地方政府提報資訊資產及弱點處置情形，確保地方政府落實資訊資產風險管控，以提出妥適因應措施，地方政府提報計畫內容應包含以下工作項目：

（一）資訊資源向上集中：

1. 朝單一資料中心為目標，縮減現有資料中心數量，建置共用資料中心，並搭配整併線路集中網路出口，大幅縮減資安防護缺口。
2. 推動內外部服務、網站及系統以雲端服務模式集中至單一資料中心，並開發共用性系統置於單一資料中心，大幅縮減所屬機關同性質之服務、網站及系統數量，避免資源重複投入，提升資訊資源及資安(訊)人力運用效率。

（二）精進資安防護能量：

1. 推動資通安全責任等級 C 級以上機關導入資訊系統弱點通報系統(Vulnerability Alert and Notification System, VANS)，協助所屬機關落實資訊資產盤點與風險評估，以自動化方式進行弱點評估，以利後續訂定弱點修補計畫。
2. 推動資通安全責任等級 B 級以上機關導入端點偵測及應變機制(EDR)，針對端點設備持續偵測異常行為或惡意程式活動，進行分析提供人員早期預警處置，避免資安事件的發生。

（三）滲透測試及紅藍軍攻防演練：推動進行擴大資安防護之滲透測試及紅藍軍攻防演練，強化地方政府資安基礎環境並培育資安人才，達成資安人才之產學交流。

（四）鼓勵弱勢性別參與措施：鼓勵弱勢性別參與資安防護相關產業及教育訓練，並於後續報送相關成果時檢附性別參與統計資料。

三、達成目標之限制、執行時可能遭遇之困難、瓶頸與解決的方式或對策

本計畫規劃以補助型計畫方式辦理，徵求地方政府提案，提案補助經費將依實際需求審查後核實給予，並依據「行政院補助地方政府強化資通安全防護作業要點」辦理，亦得不定期進行查訪及經費查核，計畫執行期滿後繳交全程執行總報告。

另本計畫採經費分攤原則，依行政院主計總處公布之地方政府財力級次給予不同補助比率，如下表：

財力級次	地方政府	補助比率
第一級	臺北市	50%
第二級	新北市、桃園市	60%
第三級	臺中市、臺南市、高雄市、新竹縣、新竹市、嘉義市、金門縣	70%
第四級	宜蘭縣、彰化縣、南投縣、雲林縣、基隆市	80%
第五級	苗栗縣、嘉義縣、屏東縣、臺東縣、花蓮縣、澎湖縣、連江縣	90%

四、與以前年度差異說明

本計畫係從 112-113 年執行，無 110-111 年度之階段性目標。

五、跨部會署合作說明

本計畫無跨部會署合作。

六、與本計畫相關之其他預算來源、經費及工作項目

本計畫除各縣市除配合中央款按比例編列自籌款外，無其他相關預算來源。

肆、前期重要效益成果說明

一、分年度重要執行成果

「強化政府基層機關資安防護及區域聯防計畫」(106 年至 109 年)，該

計畫分年度執行成果如下：

年	執行成果
106 年-107 年	1. 建立資安情資分享機制：分享資安防護規則與攻擊活動訊息，當發生大規模之網路攻擊時(如 DDoS、勒索軟體、蠕蟲發作等)，即時通知所屬及鄰近縣市進行預防或增設阻擋規則。 2. 資安教育訓練與經驗交流：定期舉辦資安事件處理之技術交流研討及區域性教育訓練。 3. 導入政府組態基準並汰換（含擴充或更新）基層機關7年以上電腦主機及資安防護設備
108 年-109 年	1. 完善地方政府區域聯防體系：以6個直轄市為核心，結合周邊鄰近縣市推動區域聯防，建立 SOC(事前監控)、CERT(事中通報)，與 ISAC(事後分享)等機制，進行相關資安監控、即時應處及情資分享，整體提升區域內的資安防護能量。 2. A、B 級機關優先導入政府組態基準(GCB)：配合資通安全管理法(以下簡稱資安法)應辦事項之要求，A、B 級機關應導入 GCB，截至109年底，各縣市政府 A 級機關及 B 級機關已全數導入，並藉由導入 GCB，降低終端設備的資安威脅，完備縱深防禦。 3. 汰換基層機關7年以上資訊軟硬體設備：為避免因老舊電腦及相關資訊設備無法適時更新，成為機關資訊安全的破口，提升資安自主產品使用，採購國產品個人電腦比例100 %，其他設備採購國產品比例亦超過50%。 4. 完善資安基礎環境：透過資安法的推動，使相關資安作為有所依據，另進行相關的產官學合作，如：新北市政府與資安公司合作建置攻擊趨勢感知系統，偵測外部與內部惡意網路攻擊；嘉義縣政府與中正大學合作，針對縣府全球資訊網進行滲透測試，由資安公司

	協助提供相關檢測工具與流程文件；臺中市政府舉辦3場資安技術交流，以國內外資安最新案例為借鏡分享討論。

二、里程碑達成情形

「強化政府基層機關資安防護及區域聯防計畫」(106 年至 109 年)，里程碑達成情形如下：

年	里程碑達成情形
106 年-107 年	1. 完成區域 ISAC 的建置。 2. 導入政府組基準比例(A、B 級)60%。 3. 提升國內資通訊產品使用率 10%。
108 年-109 年	1. 完成建置資安監控機制二線 SOC。 2. 區域聯防涵蓋範圍達 81.62%。 3. 導入政府組基準比例(A、B 級)100%。 4. 個人電腦國產品採購比例 100%。 5. 其他國產品採購比例 62.99%。

三、可量化經濟效益

「強化政府基層機關資安防護及區域聯防計畫」(106 年至 109 年)，該計畫屬其他效益(科技政策管理)非經濟效益。

四、不可量化經濟效益

「強化政府基層機關資安防護及區域聯防計畫」(106 年至 109 年)，該計畫屬其他效益(科技政策管理)非經濟效益。

伍、預期效益及效益評估方式規劃

地方政府經費、人力有限，致資安防護水準不同，爰本處 106-109 年即推動區域聯防架構，以直轄市為核心，結合鄰近縣市共同組成防護網，以精進整體資安防護，本計畫係延續區域聯防的架構概念，協助地方政府持續強化資安防護，精進產學合作，研析資安技術，預期效益重點說明如下：

1. 推動地方政府資訊資源向上集中：建置共用資料中心，推廣共用系統，整併網路集中出口，集中建置整體資安防護，以有效人力、資源共用。
2. 精進地方政府資安防護能量：主要完成資通安全 C 級以上機關導入

VANS 及 B 級以上機關導入 EDR，達成法遵要求事項，藉由 VANS 定期掌握地方政府 C 級以上的弱點情形。

3. 推動滲透測試及紅藍軍攻防演練：透由地方政府、資安業界及在地學界合作，進行相關資安技術檢測、防護及驗證等交流。

效益評估方式，將依依「行政院補助地方政府強化資通安全防護作業要點」定期進行管考，並於結案提供成果報告以了解效益情形，並透過 VANS 了解地方政府是否有配合定期資料上傳，持續追蹤效益。

陸、自我挑戰目標

本計畫目標項目：達成地方政府資料中心減量，朝單一資料中心為目標，原預期關鍵成果為計畫執行機關完成所屬機關資料中心減量，每年累計 10 個資料中心向上集中至計畫執行機關，挑戰目標將為每年累計 15 個資料中心向上集中至計畫執行機關。

柒、經費需求/經費分攤/槓桿外部資源

經費需求表(B005)

單位：千元

部會細計名稱	計畫屬性	112年度			113年度			114年度(8月)		
		小計	經常支出	資本支出	小計	經常支出	資本支出	小計	經常支出	資本支出
府層關安動禦畫/政基機資主防計(12)	8.科技政策規劃與管理	460,000	233,182.530	226,817.470	460,000	232,135.850	227,864.150			

112 年度經費需求表

經費需求說明

本計畫採資訊資源向上集中策略，透過經費補助計畫帶動地方政府資通服務整合並提升資訊資源及資安(訊)人力運用效率，聚焦機關資通服務及資安防護作業，有效精進地方政府資安防護能量，全程(112-113 年)經費預估 9.2 億元，每年 4.6 億元。

112 年度經費需求表

單位：千元

計畫名稱	細部計畫重點描述	主要績效指標 KPI	112 年度						
			小計	經常支出			資本支出		
				人事費	材料費	其他費用	土地建築	儀器設備	其他費用
政府基層機關資安主動防禦計畫(1 / 2)	一、推動地方政府資訊資源向上集中：透過資訊資源向上集中，提升地方政府資訊資源及資安(訊)人力運用效率，減少資源重複投資。 二、精進地方政府資安防護能量：配合資訊資源向上集中之必要資安防護需求，並推動導入資訊系統弱點通報機制(VANS)、端點偵測及應變機制(EDR)等資通安全管理法所訂應辦事項。 三、推動滲透測試及紅藍軍攻防演練：與大專院校或資安業者合作，結合在學理論與產業經	1-1 計畫執行機關完成所屬機關資料中心減量，降低線路分散程度達 5%。 2-1 符合資通安全責任等	460,000			233,182.530			226,817.470

	驗，實證政府資安防護，資安學子做中學，進而培育未來所需資安人才。	級C級之地方政府均導入資訊系統弱點通報機制(VANS)。 2-2 符合資通安全責任等級B級之地方政府均導入端點偵測及應變機制(EDR)。 2-3 導入VANS之地方政府機關設備所發現CVSS 7分以上資安弱點於1週內完成處置達70%。 3-1 與國內大專院校合作，培訓人才至少50人。 3-2 推動紅藍							

		隊演練或資安檢測至少6案，協助地方政府改善資安防護。								

113 年度經費需求表

經費需求說明

本計畫採資訊資源向上集中策略，透過經費補助計畫帶動地方政府資通服務整合並提升資訊資源及資安(訊)人力運用效率，聚焦機關資通服務及資安防護作業，有效精進地方政府資安防護能量，全程(112-113 年)經費預估 9.2 億元，每年 4.6 億元。

113 年度經費需求表

單位：千元

計畫名稱	細部計畫重點描述	主要績效指標 KPI	113 年度						
			小計	經常支出			資本支出		
				人事費	材料費	其他費用	土地建築	儀器設備	其他費用
政府基層機關資安主動防禦計畫（2 / 2）	一、推動地方政府資訊資源向上集中：透過資訊資源向上集中，提升地方政府資訊資源及資安(訊)人力運用效率，減少資源重複投資。 二、精進地方政府資安防護能量：配合資訊資源向上集中之必要資安防護需求，並推動導入資訊系統弱點通報機制(VANS)、端點偵測及應變機制(EDR)等資通安全管理法所訂應辦事項。 三、推動滲透測試及紅藍軍攻防演練：	1-1 計畫執行機關完成所屬機關資料中心減量，降低線路分散程度達 10%。 2-1 符合資通安全責	460,000			232,135.850			227,864.150

	與大專院校或資安業者合作，結合在學理論與產業經驗，實證政府資安防護，資安學子做中學，進而培育未來所需資安人才。	任等級B級之地方政府依資通安全管理法主管機關指定之方式提交端點偵測及應變機制(EDR)偵測資料。 2-2 導入VANS之地方政府機關設備所發現CVSS 7分以上資安弱點於1週內完成處置達75%。 3-1 與國內大專院校合作，培訓人才累							

		計至少 100 人。 3-2 推動紅藍隊演練或資安檢測累計至少 12 案，協助地方政府改善資安防護。							

經費分攤表(B008)

［無經費分攤表］

捌、儀器設備需求

本計畫係補助地方政府辦理資安作業，無儀器設備需求。

玖、就涉及公共政策事項，是否適時納入民眾參與機制之說明

無。

拾、附錄

一、政府科技發展計畫自評結果(A007)

(一)　計畫名稱：政府基層機關資安主動防禦計畫
審議編號：112-3601-09-20-01
計畫類別：前瞻基礎建設計畫

(二)自評委員：__李允中、許建隆_____ _____

日期：111 年 2 月 20 日

(三)審查意見及回復：
(應依據計畫可行性、過去績效、執行優先性、預算額度等，進行評估及建議，自評形式及次數請自行斟酌)

序號	審查意見	回復說明
1	建議能說明地方政府有哪些資訊要集中、哪些系統要共用，其根據是什麼？	資訊資源向上集中主要考量同性質，有一致性處理規範為主，依 110 年 12 月 7 日行政院國家資通安全會報第 38 次委員會議(擴大會議)，共用行政資訊系統區分行政業務系統及行政輔助系統 2 類，行政業務系統由其主管機關依法定職掌，已訂定全國處理標準；具有一致性處理規範之行政輔助系統由業務主管機關訂定 SOP 要求各機關遵循辦理，另針對無一致性處理規範之行政輔助系統，以部會為單位，建立一致性處理規範，推動共用性資訊系統或採用商業雲端服務，考量地方政府作業現況，建議優先推動電子郵件等，提供所屬機關使用，以減少重覆之資安防護作業。惟各機關可考量自身及所屬情況，適度評估優先建置對象。
2	建議在導入C級以上機關 VANS 部分，可以建立一套導入的 SOP。	有關導入 VANS 的執行方式已訂定一套導入作業流程供機關參考，將導入作業流程分為五大作業(資訊資產與已安裝 KBID 更新作業、資訊資產與已安裝 KBID 盤點作業、資訊資產與已安裝 KBID 正規畫作業、資訊資產與已安裝 KBID 登錄作業及弱點通知與修補作業)供機關導入參考，相關資訊已置於行政院國家資通安全會報技術服務中心網站，

		政府機關資安弱點通報機制(VANS)專區之「教育訓練教材」網頁。(https://www.nccst.nat.gov.tw/Vans?lang=zh)
3	建議在導入EDR部分，可以建立一套導入的SOP。	EDR的導入主要是服務導入，由各廠商依其產品特性有所不同，並由機關考量自身情形評估導入範圍，暫難訂定SOP；惟本處已要求各機關應提交EDR資料予主管機關，其相關資訊已置於行政院國家資通安全會報技術服務中心網站，端點偵測及應變機制(EDR)專區之「相關文件與表單」網頁。
4	有關效益評估的管考，建議能提出一套系統性的機制，而非僅是了解地方政府是否有配合定期資料上傳而已。	本計畫有關效益評估機制除了請機關定期提報資料外，另於執行期間會安排實地訪視，了解機關的實際執行情形及效益，該部分於前瞻一、二期補助地方政府計畫皆有執行，已有一套評估機制，本次導入VANS及EDR部分，因有統一資料收容，亦可透由系統了解機關導入情形，以VANS為例，機關可掌握受弱點影響資產數量情形。
5	計畫過去執行成佳，此次政府基層機關資安主動防禦計畫可基於延續過去執行成果，持續強化資安防禦工作，值得肯定與支持。	感謝委員肯定。
6	計畫推動地方政府資訊資源向上集中，可有效提升地方政府資訊資源及資安(訊)人力運用效率，減少資源重複投資，實屬很好的政策方向	資訊資源向上集中，主要係往縣市政府集中，期能達到由縣市政府維運，進行資安控管、資料治理、統籌維運、資安事件通報與處置等，另縣市政府因資安(訊)人力有限，各機關多會事先進行溝通確認，降低跨多單位、多系統以及多維運團隊的狀況，並釐清相關權責歸屬。

	與作為。資訊資源向上集中過程，因涉跨多單位、多系統以及多維運團隊等，建議宜確立責任權責區分與管理、資料治理與維運安全、資安事件通報與處置等管理與溝通機制。	
7	計畫績效指標 2-1 與 2-2 將配合資訊資源向上集中之必要資安防護需求，規劃資訊系統弱點通報機制(VANS)與端點偵測及應變機制(EDR)，應可有效提昇資安防護能量。建議後續宜重視此管考與稽核機制，以期發揮主動禦之實效。	有關計畫績效指標 2-1 與 2-2 之管考與稽核，除要求地方政府定期回報外，可透過 VANS 定期追蹤機關是否有將盤點資訊上傳,並確認弱點影響情形及是否有改善，另 EDR 則透由機關是否有上傳監控資訊至主管機關指定位置,從而了解實際執行情形。
8	計畫績效指標 3-1 將與國內大專院校合作，培訓人才至少 30 人次，對於我國資安人才	針對計畫績效指標 3-1 與國內大專院校合作，主要以資安相關主題為主,由地方政府搭配國內大專院校協助培育當地所需資安人才;本處前於 108 至 109 年間，亦曾透由前瞻計畫補助地方政府推動該項業務，相關縣市(如高雄)已有與業界、學界合作之經驗，由業界帶領學生進行攻防演練，進行做中

	之培訓有實質助益。建議宜考量實務合作議題、培訓與輔導機制，以及後續人才應用情形等，以期提高我國資安人才能量。	學培訓，培訓之學生為業界所採用。
9	計畫績效指標3-2將推動紅藍隊演練或資安檢測至少6案，此對攻防實務資禦工作之檢視與強化有很大助益。建議重視演練或資安檢測結果之檢討與管考作為，作為政府基層機關資安主動防禦之持續精進參考。	紅藍隊演練及資安檢測皆有對應的報告及建議,後續機關應依該建議事項進行強化資安防禦,並可將對應建議提供給其他縣市參考。

二、中程個案計畫自評檢核表(請以正本掃描上傳)

檢視項目	內 容 重 點 (內容是否依下列原則撰擬)	主辦機關		主管機關		備註
		是	否	是	否	
1.計畫書格式	(1)計畫內容應包括項目是否均已填列(「行政院所屬各機關中長程個案計畫編審要點」(以下簡稱編審要點)第5點、第12點)	✓				
	(2)延續性計畫是否辦理前期計畫執行成效評估，並提出總結評估報告(編審要點第5點、第13點)	✓				
	(3)是否依據「跨域加值公共建設財務規劃方案」之精神提具相關財務策略規劃檢核表？並依據各類審查作業規定提具相關書件		✓			
2.民間參與可行性評估	是否填寫「促參預評估檢核表」評估(依「公共建設促參預評估機制」)		✓			
3.經濟及財務效益評估	(1)是否研提選擇及替代方案之成本效益分析報告(「預算法」第34條)	✓				
	(2)是否研提完整財務計畫	✓				
4.財源籌措及資金運用	(1)經費需求合理性(經費估算依據如單價、數量等計算內容)	✓				
	(2)資金籌措：依「跨域加值公共建設財務規劃方案」精神，將影響區域進行整合規劃，並將外部效益內部化		✓			
	(3)經費負擔原則： a.中央主辦計畫：中央主管相關法令規定 b.補助型計畫：中央對直轄市及縣(市)政府補助辦法、依「跨域加值公共建設財務規劃方案」之精神所擬訂各類審查及補助規定	✓				
	(4)年度預算之安排及能量估算：所需經費能否於中程歲出概算額度內容納加以檢討，如無法納編者，應檢討調減一定比率之舊有經費支應；如仍有不敷，須檢附以前年度預算執行、檢討不經濟支出及自行檢討調整結果等經費審查之相關文件	✓				
	(5)經資比1：2(「政府公共建設計畫先期作業實施要點」第2點)		✓			
	(6)屬具自償性者，是否透過基金協助資金調度		✓			
5.人力運用	(1)能否運用現有人力辦理	✓				
	(2)擬請增人力者，是否檢附下列資料： a.現有人力運用情形 b.計畫結束後，請增人力之處理原則 c.請增人力之類別及進用方式 d.請增人力之經費來源		✓			

檢視項目	內　容　重　點 （內容是否依下列原則撰擬）	主辦機關		主管機關		備註
		是	否	是	否	
6.營運管理計畫	是否具務實及合理性(或能否落實營運)	✓				
7.土地取得	(1)能否優先使用公有閒置土地房舍		✓			
	(2)屬補助型計畫，補助方式是否符合規定(中央對直轄市及縣(市)政府補助辦法第10條)		✓			
	(3)計畫中是否涉及徵收或區段徵收特定農業區之農牧用地		✓			
	(4)是否符合土地徵收條例第3條之1及土地徵收條例施行細則第2條之1規定		✓			
	(5)若涉及原住民族保留地開發利用者，是否依原住民族基本法第21條規定辦理		✓			
8.風險評估	是否對計畫內容進行風險評估	✓				
9.環境影響分析(環境政　策評估)	是否須辦理環境影響評估		✓			
10.性別影響評估	是否填具性別影響評估檢視表	✓				
11.無障礙及通用設計影響評估	是否考量無障礙環境，參考建築及活動空間相關規範辦理		✓			
12.高齡社會影響評估	是否考量高齡者友善措施，參考WHO「高齡友善城市指南」相關規定辦理		✓			
13.涉及空間規劃者	是否檢附計畫範圍具座標之向量圖檔		✓			
14.涉及政府辦公廳舍興建購置者	是否納入積極活化閒置資產及引進民間資源共同開發之理念		✓			
15.跨機關協商	(1)涉及跨部會或地方權責及財務分攤，是否進行跨機關協商		✓			
	(2)是否檢附相關協商文書資料		✓			
16.依碳中和概念優先選列節能減碳指標	(1)是否以二氧化碳之減量為節能減碳指標，並設定減量目標		✓			
	(2)是否規劃採用綠建築或其他節能減碳措施		✓			
	(3)是否檢附相關說明文件		✓			
17.資通安全防護規劃	資訊系統是否辦理資通安全防護規劃	✓				

主辦機關核章：承辦人　　單位主管　　首長

主管部會核章：研考主管　　會計主管　　首長

說明：1.中程個案計畫，應由機關副首長召集有關單位進行自評後，報請機關首長核定。自評作業，得諮詢專家、學者、相關機關或團體意見，並應填列中程個案計畫自評檢核表，納入計畫書。

2.此表需經由長官核章後方可上傳。

三、性別影響評估檢視表

中長程個案計畫性別影響評估檢視表【一般表】

【第一部分】：本部分由機關人員填寫

【填表說明】各機關使用本表之方法與時機如下：

一、計畫研擬階段

（一）請於研擬初期即閱讀並掌握表中所有評估項目；並就計畫方向或構想徵詢作業說明第三點所稱之性別諮詢員（至少 1 人），或提報各部會性別平等專案小組，收集性別平等觀點之意見。

（二）請運用本表所列之評估項目，將性別觀點融入計畫書草案：

1. 將性別目標、績效指標、衡量標準及目標值納入計畫書草案之計畫目標章節。
2. 將達成性別目標之主要執行策略納入計畫書草案之適當章節。

二、計畫研擬完成

（一）請填寫完成【第一部分－機關自評】之「壹、看見性別」及「貳、回應性別落差與需求」後，併同計畫書草案送請性別平等專家學者填寫【第二部分－程序參與】，宜至少預留 1 週給專家學者（以下稱為程序參與者）填寫。

（二）請參酌程序參與者之意見，修正計畫書草案與表格內容，並填寫【第一部分－機關自評】之「參、評估結果」後通知程序參與者審閱。

三、計畫審議階段：請參酌行政院性別平等處或性別平等專家學者意見，修正計畫書草案及表格內容。

四、計畫執行階段：請將性別目標之績效指標納入年度個案計畫管制並進行評核；如於實際執行時遇性別相關問題，得視需要將計畫提報至性別平等專案小組進行諮詢討論，以協助解決所遇困難。

註：本表各欄位除評估計畫對於不同性別之影響外，亦請關照對不同性傾向、性別特質或性別認同者之影響。

計畫名稱：

主管機關 （請填列中央二級主管機關）	行政院資通安全處	**主辦機關（單位）** （請填列擬案機關／單位）	行政院資通安全處

1. **看見性別：**檢視本計畫與性別平等相關法規、政策之相關性，並運用性別統計及性別分析，「看見」本計畫之性別議題。

評估項目	評估結果
1-1【請說明本計畫與性別平等相關法規、政策之相關性】	因應國際性別主流化潮流，推動性別平等政策綱領，建構性

性別平等相關法規與政策包含憲法、法律、性別平等政策綱領及消除對婦女一切形式歧視公約（CEDAW）可參考行政院性別平等會網站（https://gec.ey.gov.tw）。	別友善職場環境，鼓勵女性參與決策，於各層級合議式決策機制(委員會)內，應不低於1/3 比例，以追求平等參與、破除性別隔離，讓男女能平等參與決策，減少因性別而帶來的知識與技術落差，並鼓勵女性成為意見領袖，重視女性與弱勢者的經驗、知識和價值。
評估項目	**評估結果**
1-2【請蒐集與本計畫相關之性別統計及性別分析（含前期或相關計畫之執行結果），並分析性別落差情形及原因】 請依下列說明填寫評估結果： a.歡迎查閱行政院性別平等處建置之「性別平等研究文獻資源網」（https://www.gender.ey.gov.tw/research/）、「重要性別統計資料庫」(https://www.gender.ey.gov.tw/gecdb/)（含性別分析專區）、各部會性別統計專區、我國婦女人權指標及「行政院性別平等會—性別分析」(https://gec.ey.gov.tw)。 b.性別統計及性別分析資料蒐集範圍應包含下列3類群體： ①**政策規劃者**（例如:機關研擬與決策人員；外部諮詢人員）。 ②**服務提供者**（例如:機關執行人員、委外廠商人力）。 ③**受益者**（或使用者）。 c.前項之性別統計與性別分析應盡量顧及不同性別、性傾向、性別特質及性別認同者，探究其處境或需求是否存在差異，及造成差異之原因；並宜與年齡、族群、地區、障礙情形等面向進行交叉分析（例如：高齡身障女性、偏遠地區新住民女性），探究在各因素交織影響下，是否加劇其處境之不利，並分析處境不利群體之需求。前述經分析所發現之處境不利群體及其需求與原因，應於後續【1-3找出本計畫之性別議題】，及【貳、回應性別落差與需求】等項目進行評估說明。 d.未有相關性別統計及性別分析資料時，請將「強化與本計畫相關的性別統計與性別分析」列入本計畫之性別目標（如2-1之ｆ）。	1.本計畫決策人員共3人，女性有1人占比33%，已超過1/3。 2.本計畫機關執行人員為各地方政府承辦，現有22人，其中女性有8人占比36.4%，已超過1/3。 3.本計畫係屬於補助型計畫，計畫完成後，受益對象為地方政府所有同仁，並不以特定性別、性傾向或性別認同者為受益對象。 4.過去五年(104年至108年)資訊通訊科技領域之畢業生男女性別比率約為7 比3。本計畫舉辦人才培訓活動時，將建議各執行機關鼓勵女性參與，且參與率應不低於30%。
評估項目	**評估結果**

1-3【請根據 1-1 及 1-2 的評估結果，找出本計畫之性別議題】 性別議題舉例如次： **a. 參與人員** 政策規劃者或服務提供者之性別比例差距過大時，宜關注職場性別隔離（例如：某些職業的從業人員以特定性別為大宗、高階職位多由單一性別擔任）、職場性別友善性不足（例如：缺乏防治性騷擾措施；未設置哺集乳室；未顧及員工對於家庭照顧之需求，提供彈性工作安排等措施），及性別參與不足等問題。 **b. 受益情形** ①受益者人數之性別比例差距過大，或偏離母體之性別比例，宜關注不同性別可能未有平等取得社會資源之機會（例如:獲得政府補助；參加人才培訓活動），或平等參與社會及公共事務之機會（例如:參加公聽會/說明會）。 ②受益者受益程度之性別差距過大時（例如:滿意度、社會保險給付金額），宜關注弱勢性別之需求與處境（例如:家庭照顧責任使女性未能連續就業，影響年金領取額度）。 **c. 公共空間** 公共空間之規劃與設計，宜關注不同性別、性傾向、性別特質及性別認同者之空間使用性、安全性及友善性。 ①使用性：兼顧不同生理差異所產生的不同需求。 ②安全性：消除空間死角、相關安全設施。 ③友善性：兼顧性別、性傾向或性別認同者之特殊使用需求。 **d. 展覽、演出或傳播內容** 藝術展覽或演出作品、文化禮俗儀典與觀念、文物史料、訓練教材、政令/活動宣導等內容，宜注意是否避免複製性別刻板印象、有助建立弱勢性別在公共領域之可見性與主體性。 **e. 研究類計畫** 研究類計畫之參與者（例如:研究團隊）性別落差過大時，宜關注不同性別參與機會、職場性別友善性不足等問題；若以「人」為研究對象，宜注意研究過程及結論與建議是否納入性別觀點。	1. 本計畫決策人員與機關執行人員女性比例超過 1/3，無性別參與不足等問題。 2. 本計畫係屬於補助型計畫，計畫完成後，受益對象為地方政府全體同仁，並不以特定性別、性傾向或性別認同者為受益對象。 3. 本計畫舉辦人才培訓活動時，將建議各執行機關於公共空間營造性別友善環境，並鼓勵弱勢性別族群參與。

貳、回應性別落差與需求：針對本計畫之性別議題，訂定性別目標、執行策略及編列相關預算。

評估項目	評估結果

2-1【請訂定本計畫之性別目標、績效指標、衡量標準及目標值】 請針對 1-3 的評估結果，擬訂本計畫之性別目標，並為衡量性別目標達成情形，請訂定相應之績效指標、衡量標準及目標值，並納入計畫書草案之計畫目標章節。性別目標宜具有下列效益： **a. 參與人員** [1]促進弱勢性別參與本計畫規劃、決策及執行，納入不同性別經驗與意見。 [2]加強培育弱勢性別人才，強化其領導與管理知能，以利進入決策階層。 [3]營造性別友善職場，縮小職場性別隔離。 **b. 受益情形** ① 回應不同性別需求，縮小不同性別滿意度落差。 ② 增進弱勢性別獲得社會資源之機會（例如:獲得政府補助；參加人才培訓活動）。 ③ 增進弱勢性別參與社會及公共事務之機會（例如:參加公聽會/說明會，表達意見與需求）。 **c. 公共空間** 回應不同性別對公共空間使用性、安全性及友善性之意見與需求，打造性別友善之公共空間。 **d. 展覽、演出或傳播內容** ① 消除傳統文化對不同性別之限制或僵化期待，形塑或推展性別平等觀念或文化。 ② 提升弱勢性別在公共領域之可見性與主體性（如作品展出或演出；參加運動競賽）。 **e. 研究類計畫** ① 產出具性別觀點之研究報告。 ② 加強培育及延攬環境、能源及科技領域之女性研究人才，提升女性專業技術研發能力。 f. 強化與本計畫相關的性別統計與性別分析。 g. 其他有助促進性別平等之效益。	□有訂定性別目標者，請將性別目標、績效指標、衡量標準及目標值納入計畫書草案之計畫目標章節，並於本欄敘明計畫書草案之頁碼： ■未訂定性別目標者，請說明原因及確保落實性別平等事項之機制或方法。 1.因本計畫屬於補助型計畫，主要補助地方政府採購相關資安設備及服務。計畫規劃階段決策人員及機關執行人員女性占比亦超過 1/3，且計畫完成後，受益對象為地方政府全體同仁，並不以特定性別、性傾向或性別認同者為受益對象，故本次不另外訂定性別目標。 2.舉辦人才培訓活動時，將建議各執行機關了解弱勢性別族群之需求，營造性別友善環境，鼓勵弱勢性別族群參與。
評估項目	**評估結果**
2-2【請根據 2-1 本計畫所訂定之性別目標，訂定執行策略】 請參考下列原則，設計有效的執行策略及其配套措施： **a. 參與人員**	□有訂定執行策略者，請將主要的執行策略納入計畫書草案之適當章節，並於本欄敘明計畫書草案之頁碼：

① 本計畫研擬、決策及執行各階段之參與成員、組織或機制（如相關會議、審查委員會、專案辦公室成員或執行團隊）符合任一性別不少於三分之一原則。

② 前項參與成員具備性別平等意識/有參加性別平等相關課程。

b.宣導傳播

① 針對不同背景的目標對象（如不諳本國語言者；不同年齡、族群或居住地民眾）採取不同傳播方法傳布訊息（例如：透過社區公布欄、鄰里活動、網路、報紙、宣傳單、APP、廣播、電視等多元管道公開訊息，或結合婦女團體、老人福利或身障等民間團體傳布訊息）。

② 宣導傳播內容避免具性別刻板印象或性別歧視意味之語言、符號或案例。

③ 與民眾溝通之內容如涉及高深專業知識，將以民眾較易理解之方式，進行口頭說明或提供書面資料。

c.促進弱勢性別參與公共事務

① 計畫內容若對人民之權益有重大影響，宜與民眾進行充分之政策溝通，並落實性別參與。

② 規劃與民眾溝通之活動時，考量不同背景者之參與需求，採多元時段辦理多場次，並視需要提供交通接駁、臨時托育等友善服務。

③ 辦理出席民眾之性別統計；如有性別落差過大情形，將提出加強蒐集弱勢性別意見之措施。

④ 培力弱勢性別，形成組織、取得發言權或領導地位。

d.培育專業人才

① 規劃人才培訓活動時，納入鼓勵或促進弱勢性別參加之措施（例如:提供交通接駁、臨時托育等友善服務；優先保障名額；培訓活動之宣傳設計，強化歡迎或友善弱勢性別參與之訊息；結合相關機關、民間團體或組織，宣傳培訓活動）。

② 辦理參訓者人數及回饋意見之性別統計與性別分析，作為未來精進培訓活動之參考。

③ 培訓內涵中融入性別平等教育或宣導，提升相關領域從業人員之性別敏感度。

④ 辦理培訓活動之師資性別統計，作為未來師資邀請或師資培訓之參考。

■未訂執行策略者，請說明原因及改善方法：

1.因本計畫屬於補助型計畫，主要補助地方政府採購相關資安設備及服務。計畫規劃階段決策人員及機關執行人員女性占比亦超過1/3，且計畫完成後，受益對象為地方政府全體同仁，並不以特定性別、性傾向或性別認同者為受益對象，故本次不另外訂定性別目標及相關策略。

2.舉辦人才培訓活動時，將建議各執行機關了解弱勢性別族群之需求，營造性別友善環境，鼓勵弱勢性別族群參與。

e.具性別平等精神之展覽、演出或傳播內容 ① 規劃展覽、演出或傳播內容時，避免複製性別刻板印象，並注意創作者、表演者之性別平衡。 ② 製作歷史文物、傳統藝術之導覽、介紹等影音或文字資料時，將納入現代性別平等觀點之詮釋內容。 ③ 規劃以性別平等為主題的展覽、演出或傳播內容（例如:女性的歷史貢獻、對多元性別之瞭解與尊重、移民女性之處境與貢獻、不同族群之性別文化）。 **f.建構性別友善之職場環境** 委託民間辦理業務時，推廣促進性別平等之積極性作法（例如：評選項目訂有友善家庭、企業托兒、彈性工時與工作安排等性別友善措施；鼓勵民間廠商拔擢弱勢性別優秀人才擔任管理職），以營造性別友善職場環境。 **g.具性別觀點之研究類計畫** ①研究團隊成員符合任一性別不少於三分之一原則，並積極培育及延攬女性科技研究人才；積極鼓勵女性擔任環境、能源與科技領域研究類計畫之計畫主持人。 ②以「人」為研究對象之研究，需進行性別分析，研究結論與建議亦需具性別觀點。	
評估項目	**評估結果**
2-3【請根據2-2本計畫所訂定之執行策略，編列或調整相關經費配置】 各機關於籌編年度概算時，請將本計畫所編列或調整之性別相關經費納入性別預算編列情形表，以確保性別相關事項有足夠經費及資源落實執行，以達成性別目標或回應性別差異需求。	□有編列或調整經費配置者，請說明預算額度編列或調整情形： ■未編列或調整經費配置者，請說明原因及改善方法： 因本計畫屬於補助型計畫，主要補助地方政府採購相關資安設備及服務，且計畫完成後，受益對象為地方政府全體同仁，並不以特定性別、性傾向或性別認同者為受益對象，故未編列性別相關事項經費。

【注意】填完前開內容後，請先依「填表說明二之（一）」辦理【第二部分－程序參與】，再續填下列「參、評估結果」。

參、評估結果

請機關填表人依據【第二部分－程序參與】性別平等專家學者之檢視意見，提出綜合說明及參採情形後通知程序參與者審閱。

3-1 綜合說明	本計畫乃針對補助地方政府採購相關資安設備及服務，委員主要意見係涉及人才培訓部分，其參與之性別比例可無須強制規定；但未來執行時，仍宜留意避免複製性別刻板印象，並應營造性別友善環境，使不同性別均有獲得資訊及平等參與之機會，鼓勵弱勢性別族群參與，因各地方政府均已建置性別統計專區或性別主流化專區，以致力於營造性別友善環境，爰無計畫書調整之必要，後續於計畫執行時請地方政府注意該事項。	
3-2 參採情形	3-2-1 說明採納意見後之計畫調整（請標註頁數）	無
	3-2-2 說明未參採之理由或替代規劃	無

3-3 通知程序參與之專家學者本計畫之評估結果：

已於 111 年 2 月 21 日將「評估結果」及「修正後之計畫書草案」通知程序參與者審閱。

- **填表人姓名：戴全裕　職稱：分析師　電話：(02)33568068**

  填表日期：110 年 02 月 13 日

- **本案已於計畫研擬初期■徵詢性別諮詢員之意見，或□提報各部會性別平等專案小組（會議日期：____年____月____日）**

- **性別諮詢員姓名：<u>顏秀慧</u>____ 服務單位及職稱：<u>財團法人台灣綠色生產力基金會法務室主任</u>身分：符合中長程個案計畫性別影響評估作業說明第三點第<u>一、三</u>款**
  （如提報各部會性別平等專案小組者，免填）

（請提醒性別諮詢員恪遵保密義務，未經部會同意不得逕自對外公開計畫草案）

【第二部分－程序參與】：由性別平等專家學者填寫

程序參與之性別平等專家學者應符合下列資格之一：

☑1.現任臺灣國家婦女館網站「性別主流化人才資料庫」公、私部門之專家學者；其中公部門專家應非本機關及所屬機關之人員（人才資料庫網址:http://www.taiwanwomencenter.org.tw/）。

□2.現任或曾任行政院性別平等會民間委員。

☑3.現任或曾任各部會性別平等專案小組民間委員。

（一）基本資料

1.程序參與期程或時間	111 年 2 月 17 日 至 111 年 2 月 20 日
2.參與者姓名、職稱、服務單位及其專長領域	顏秀慧 財團法人台灣綠色生產力基金會法務室主任 台灣大學環工所、成功大學環醫所兼任助理教授 環境法律與政策、環境工程、環境正義與性別主流化
3.參與方式	□計畫研商會議 □性別平等專案小組 ☑書面意見

（二）主要意見（若參與方式為提報各部會性別平等專案小組，可附上會議發言要旨，免填 4 至 10 欄位，並請通知程序參與者恪遵保密義務）

4.性別平等相關法規政策相關性評估之合宜性	合宜。
5.性別統計及性別分析之合宜性	合宜。 本計畫已針對政策規劃者、服務提供者（機關執行人員）及受益者分別進行性別統計及分析。 政策規劃者及服務提供者之現行比例均符合任一性別達三分之一以上之原則；受益者為地方政府所有同仁，較不受特定性別、性傾向或性別認同之影響，探究性別差異之必要性較低。 本計畫將舉辦人才培訓活動，已統計過去五年(104 年至 108 年)資訊通訊科技領域之畢業生男女性別比率，有助於瞭解日後執行時參與率之提升方向。
6.本計畫性別議題之合宜性	合宜，就本計畫之性質及內容觀之，無須設定性別議題。 1.參與人員：政策規劃者及服務提供者之性別比例已符合任一性別達三分之一以上之原則。 2.受益者受益程度較無因性別產生過大差距之情形。

7.性別目標之合宜性	合宜，就本計畫之性質及內容觀之，無須設定性別目標。 就內部參與人員而言，相關工作須具備專業技能，且現行比例已符任一性別達三分之一以上之原則。 受益者受益程度較無因性別產生過大差距之情形，無訂定性別目標之必要性及迫切性。
8.執行策略之合宜性	合宜，就本計畫之性質及內容觀之，無須設定執行策略。 本計畫以資通安全之專業科技運用為主，性質極具專業性及技術性，故涉及人才培訓部分，其參與之性別比例可無須強制規定；但未來執行時，仍宜留意避免複製性別刻板印象，並應營造性別友善環境，使不同性別均有獲得資訊及平等參與之機會，鼓勵弱勢性別族群參與。
9.經費編列或配置之合宜性	本計畫未編列性別相關經費尚屬合宜。
10.綜合性檢視意見	1.本計畫之工作內容未涉及性別議題，且已針對政策規劃者、服務提供者（機關執行人員）及受益者分別進行性別統計及分析。 2.政策規劃者及服務提供者之現行比例均符合任一性別達三分之一以上之原則;受益者為地方政府所有同仁，探究性別差異之必要性較低。 3.本計畫以資通安全之專業科技運用為主，性質極具專業性及技術性，故涉及人才培訓部分，其參與之性別比例可無須強制規定；但未來執行時，仍宜留意避免複製性別刻板印象，並應營造性別友善環境，使不同性別均有獲得資訊及平等參與之機會，鼓勵弱勢性別族群參與。
（三）參與時機及方式之合宜性	合宜。

本人同意恪遵保密義務，未經部會同意不得逕自對外公開所評估之計畫草案。

（簽章，簽名或打字皆可） 顏秀慧

四、風險管理評估檢視表

【第一部分】：計畫現有風險圖像

嚴重 (3)	計畫成果未符合原訂目標		
中度 (2)		經費未能於期限前 完全核銷作業	因疫情致使計畫相關產出 無法如期完成
輕微 (1)			
影響程度 可能性	不太可能 (1)	可能 (2)	非常可能 (3)

【第二部分】：計畫風險評估及處理彙總表

風險項目	風險情境	現有風險對策	可能影響層面	現有風險等級		現有風險值(R)=(L)x(I)	新增風險對策	殘餘風險等級		殘餘風險值(R)=(L)x(I)
				可能性(L)	影響程度(I)			可能性(L)	影響程度(I)	
計畫成果未符合原訂目標	機關規劃與執行有所落差，導致計畫成果未能符合原訂目標	透過GSTP系統管考	計畫未能達成KPI	1	3	3	辦理計畫實地訪視，即時了解機關計畫執行情形	1	1	1
經費未能於期限前完全核銷作業	機關因招標案或請款作業程序延誤，致使未能於期限前完全核銷作業	核定各機關經費之公文敘明請款期限	經費須辦理保留	2	2	4	每月統計機關請款情形，並適時通知進度落後之機關	1	2	2
因疫情致使計畫相關產出無法如期完成	因疫情導致設備採購交貨延誤或相關訓練會議無法召開，進	透過GSTP系統管考	計畫執行率落後	3	2	6	要求機關提前作業，並研議採線上方式辦理	2	1	2

風險項目	風險情境	現有風險對策	可能影響層面	現有風險等級		現有風險值(R)=(L)x(I)	新增風險對策	殘餘風險等級		殘餘風險值(R)=(L)x(I)
				可能性(L)	影響程度(I)			可能性(L)	影響程度(I)	
	而影響計畫進度						相關訓練或會議			

【第三部分】：計畫殘餘風險圖像

嚴重 (3)			
中度 (2)	經費未能於期限前 完全核銷作業		
輕微 (1)	計畫成果未符合原訂目標	因疫情致使計畫相關產出 無法如期完成	
影響程度 / 可能性	不太可能 (1)	可能 (2)	非常可能 (3)

極度風險： 0 項(0 %)

高度風險： 0 項(0 %)

中度風險： 0 項(0 %)

低度風險： 4 項(100 %)

五、政府科技發展計畫審查意見回復表(A008)

審議編號：112-3601-09-20-01
計畫名稱：政府基層機關資安主動防禦計畫
申請機關(單位)：行政院資通安全處

序號	審查意見	回復說明	修正頁碼
1	計畫延續前瞻基礎建設計畫第一期強化政府基層機關資安防護及區域聯防計畫，協助地方政府持續強化資安防護，精進產學合作，符合國家資通安全發展方案(110 年至 113 年)中「賡續推動政府資訊(安)集中共享」之措施。	感謝委員支持。	
2	推動地方政府資訊資源向上集中，可有效提升地方政府資訊資源及資安(訊)人力運用效率，減少資源重複投資；導入 VANS 有助於提升地方政府茲安防護能量；考量國際資安威脅日益嚴峻，而地方政府相關系統有其弱點，為協助地方政府資安防護永續經營，本計畫推動有其必要性及迫切性。	感謝委員支持。	
3	目標及關鍵成果部分 (1)本計畫預計在本期將所有地方政府導入 VANS，並讓所有 B 級地方政府機關導入 EDR，關鍵成果與目標明確。 (2)促進產官學合作部分，推動資安業界與在地政府與學界合作驗證，有	感謝委員支持。	

	助協助找出可能資安威脅。地方政府結合國內大專院校合作培訓資安人才對我國資安人才培育也有助益，但是其成果產出應該更明確要求，並強化計畫之各年度期中查證。 (3) 本計畫所擬定之關鍵成果與目標扣合度高，惟成果大多以操作型指標展現，不易評估其執行品質。建議本計畫預期關鍵成果中增加地方政府之執行效益(或續用前期相關執行之主要績效指標)，以利展現推動成果與亮點。 (4) 計畫目前已修正可檢核之最終效益，應搭配對各地方政府計畫成果之落實查核。 (5) 本計畫 112 年度與 113 年度之目標與預期關鍵成果大多相似或相同，建議依全程執行進度設計不同年度之目標，以展現本計畫推動之進階性及進展。		

4	執行面建議 (1)本計畫促進產官學合作部分宜與國科會學術型資安研究計畫搭配，共同串接學校研究與人才資源。 (2)本計畫主要目標之一為「精進資安防護能量」，惟各地方政府所轄之資安防護能力(技術與人力)不一，各分項/縣市計畫書中所述之作法也不相同；本計畫推動時提案單位宜加強督導或進行期中查證，並協助防護力較弱或執行力較弱的縣市完善其推動策略。 (3)減少網路攻擊介面及增加資訊流能見度是資安基礎建設，本計畫規劃之資料中心向上集中策略，可減少各地方政府在資安管理上的能量欠缺問題，藉由單一資料中心，能有效減少攻擊介面，同時將有限資源聚焦在單一資料中心的防護上，應該在政府資	感謝委員支持。	

	安基礎建設強化中落實。 (4)弱點管理與修補，資安態勢的掌控也是近年來國際資安防禦的重要策略，透過VANS機制的佈建，對於C級機關的弱點管控確有其必要性，而B級機關EDR的佈建，對於資源欠缺的地方政府，是當務之急。計畫執行單位亦針對各地方政府財務能力，訂定不同補助比例，有助於政府資源的有效運用。但須追蹤運用成效。		
5	計畫預期效益部分 (1)本計畫預期效益，集中建置整體資安防護，以有效人力、資源共用目標明確，但目前地方政府資料中心約350個以上，每年集中10個資料中心效益不大，應予提高至少減少40個以上(淨值)。 (2)推動地方政府產官學合作及實證場域部分對於	(1)推動地方政府資源向上集中，為提升資訊資源及資安人力運用效率，各機關資訊系統採縣市政府統籌維運、資安控管集中需要，惟部分機關涉全國性業務及資通系統，有個別集中需求，如地政、稅務、警政、消防等，配合實務議題，爰本計畫預計112年以逐年縮減10個	(1)2、5、6、7、8、13、22、25 (2)2、5、7、14、

	提升地方政府資安防護效益不明確，且每年培訓人才 30 人次過少，應改為人數，並請資安處補充所培育的人才的資安職能。 (3) 本計畫承接前期計畫成果，切合「資安即國安」政策方針，透過整體資安聯合防禦機制，以有效防範政府機關遭受資安攻擊之風險，規劃完整可行，切合需求。本計畫所擬定之自我挑戰目標適切可行。	資料中心為目標，並以 15 個為挑戰目標，並依委員意見將指標修正為「計畫執行機關完成所屬機關資料中心減量，降低線路分散程度」。 (2) 本計畫推動由地方政府搭配國內大專院校、業界培育資安策略面、管理面、技術面之資安職能，各縣市政府依其資安作業需求，培訓數位鑑識或網路攻防人才，有關培訓量能將依委員建議調整為人數，提升為 50 人(修正計畫第 5、8-11、17、25、27 頁)，後續視推動情形滾動檢討。	23
6	本計畫經費考量地方政府需求，以及作為院資安處轉入數位部的過渡時期作法，建議支持，但申請單位需配合以下事項： (1) 院資安處未來轉入數位部，將無法沿用行政院補助地方政府強化資通安全防護作業要點補助地方政府，需另訂要	感謝委員支持，本案計畫啟動時間為 112 年，屆時將與數位發展部併同考量相關做法，使補助作業有所依循。	

	點。 (2)不符合本計畫工作項目的地方政府提案不在補助之列，應優先刪減。		
7	本案計畫雖已修正最終效益及各年度目標，惟仍未能有效呈現防禦能力提升，僅屬於投入面指標訂定，後續仍請精進調整，並補充網路及應用韌性提升指標訂定。	指標修正為「計畫執行機關完成所屬機關資料中心減量，降低線路分散程度」，112 年指標達 5%，113 年指標達 10%，以提升網路及應用韌性。	2、5、6、7、8、13、22、25
8	請提出本案計畫後續維運之規劃說明，尤其針對未提出經費需求之地方政府。	(1)金門縣政府規劃於 112 年建置系統，後續以保固方式維運，113 年由該府自行編列經費辦理維護及營運。 (2)嘉義市政府規劃於 112 年建置系統，於 113 年將 EDR 相關成果分析以利調整改善，後續以軟體升級授權(MA)方式維運。	
9	本案計畫刪除產官學合作部分，轉為其他績效指標進行運作，包括加強滲透測試及紅藍軍攻防演練內容規劃。	本案計畫刪除產官學於實證場域合作部分，轉為擴大於滲透測試、紅藍軍攻防演練內容等強化資安規劃，引入資安人才之產學交流。	1、2、3、5、7、8、11、12、13、15、19、22、25
10	本案計畫請執行單位於文到一週內提出執行模式、工作項目及 KPI 修正內容，由科技會報辦公室會同審查委員檢視確認，並視需求另案召開專案會議。	調整政府基層機關資安主動防禦計畫執行模式、工作項目及 KPI。	2、5、6、7、8、13、14、22、23、25、26、27

11	本計畫112年與113年建議經費核定數為每年 4.6 億元。	依核定數調整計畫及各項子計畫核定經費。	4、5、21、22、25、58、附件1-6
12	本案係開放地方政府申請經費之補助型計畫，有關本計畫補助執行機關辦理培育資安人才活動部分，為改善長期以來資通訊領域人才性別落差，建議將「鼓勵弱勢性別參與措施」納入審查各執行機關提送計畫之要項，以降低科技領域人才之性別區隔；並請執行機關報送相關活動成果時，納入性別參與之統計資料，以瞭解其推動前揭衡平性別比例措施之成效，俾作為未來辦理相關培育資安人才活動之參考。	請各地方政府於計畫內加入鼓勵弱勢性別參與措施，並於報送相關活動成果時納入性別統計資料。	15

六、資安經費投入自評表(A010)

(如有填寫疑問，請逕洽行政院資安處 3356-8063)

部會			單位				
審議編號	計畫名稱	期程(年)	總經費(千元)(A)	資訊總經費(千元)(B)	資安經費(千元)(C)	比例[註1](D)	備註
112-3601-09-20-01	政府基層機關資安主動防禦計畫	2	920,000	920,000	920,000	100%	

資安經費投入項目				
項次	年度	投入項目類別[註2]	投入項目	預估經費(千元)
1	112	2-1(A1) 2-2(B1) 2-3(C3)	資訊資源向上集中、精進資安防護及滲透測試及紅藍軍攻防演練	460,000
2	113	2-1(A1) 2-2(B1) 2-3(C3)	資訊資源向上集中、精進資安防護及滲透測試及紅藍軍攻防演練	460,000
總計				920,000

備註：

1、 資安經費提撥比例係依計畫總經費(A)或資訊總經費(B)計算(可多計畫合併)，各計畫可依業務性質及實際需求於計畫執行年度分階段辦理。

1-1 109 年(含)前結束之計畫，其需達成資安經費比例(D)計算方式=(資安總經費(C)/資訊總經費(B))*100%，1 億(含)以下提撥 7%、1 億以上至 10 億(含)提撥 6%、10 億以上提撥 5%。

1-2 110-114 年(含)後結束之計畫，除前述資安經費比例，另配合行政院政策逐年提高資安經費比例至「資安產業發展行動計畫(107-114 年)」所訂 114 年預期達成目標。

2、 投入項目類別請用下列代號填寫：

2-1 系統開發

(A1) **依據資通安全管理法—資通安全責任等級分級辦法之**「資通系統防護需求分級原則」，完備「資通系統防護基準」之**各項措施。**

(A2) 推動「安全軟體發展生命週期(SSDLC)」，可參考行政院國家資通安全會報技術服務中心所訂「資訊系統委外開發 RFP 資安需求範本」。

(A3) 依據經濟部工業局所訂「行動應用 APP 安全開發指引」、「行動應用 APP 基本資安檢測基準」、「行動應用 APP 基本資安自主檢測推動制度」等，進行相關資安檢測作業。

2-2 軟硬體採購

(B1) 依據資通安全管理法—資通安全責任等級之公務機關應辦事項，建置必要之縱深防禦機制，含網路層(例如：防火牆、網站防火牆等)、主機層(例如：防毒軟體、電子郵件過濾機制等)、應用系統層等資安防護措施。

(B2) 推動國內認證/驗證規範，並將該產品通過之相關認證/驗證或符合相關規範納入建議書徵求說明書，例如：影像監控系統需符合影像監控系統相關資安標準，且經合格實驗室認證通過。

(B3) 各項設備應導入政府組態基準(Government Configuration Baseline，GCB)。

2-3 其他建議項目

(C1) 資安檢測標準研訂。

(C2) 新興資安領域(例如：5+2產業創新計畫)之資安風險與防護需求研究。

(C3) 新興資安領域之人才培育。

（C4） 編撰資安訓練教材。

其他資安相關項目(例如：推動「資安產業發展行動計畫」之四項策略-建立以需求導向之資安人才培訓體系、聚焦利基市場橋接國際夥伴、建置產品淬煉場域提供產業進軍國際所需實績、活絡資安投資市場全力拓銷國際)。

七、其他補充資料

附件 1：臺北市政府(含金門縣、連江縣、花蓮縣政府)

附件 2：新北市政府(含基隆市、宜蘭縣政府)

附件 3：桃園市政府(含新竹市、新竹縣、苗栗縣政府)

附件 4：臺中市政府(含彰化縣、南投縣政府)

附件 5：臺南市政府(含嘉義市、嘉義縣、雲林縣政府)

附件 6：高雄市政府(含屏東縣、澎湖縣、臺東縣政府)

附件 1

政府基層機關資安主動防禦之分項計畫

臺北市政府(含金門縣、連江縣、花蓮縣政府)

計畫全程：112 年 1 月至 113 年 12 月

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

現行地方政府已經由行政院前瞻基礎建設之經費挹注下，完善了各項資通安全基礎，包含以下成果：

(一)區域聯防體系縣市聯防架構，建置以臺北市政府為主，帶動花蓮縣政府、金門縣政府、連江縣政府之情資分享與資安事件監控機制。

(二)政府基準組態導入達八成以上，有效阻斷設備組態不佳造成的資安威脅。

(三)完善資安基準環境，汰換老舊作業系統，提升整體資安防護基礎能量。

(四)促進產學研合作，引進產學研資源，豐富政府機關資安資源整合。

惟經由107-111年推動後，地方政府尚需精進改善以下議題：

(一)地方政府因資訊發展期程不一，機房與應用系統分散管理，造成資訊資源與人力重複投注，資安防護能量亦分散管理，造成偵測、防護與阻斷速度不佳，相關風險控管亦因不同單位管理而有不同強度水準，無法有效均一化資安要求與稽核管控。

(二)資安經費長期偏低，地方財政持續拮据，地方政府資訊預算仍難受重視，無法滿足持續增長的數位化需求與資安防護要求。

(三)端點防護整合不佳，異質端點防護軟體持續累加安裝，除造成端點效能降低外，情資分享與整合機制不佳，亦造成情資向上集中、向下清查應變查處之速度緩慢。

(四)異質資安設備眾多，SOC已協助進行關聯分析並通報，相關日誌調閱調查至處置阻斷攻擊耗時費力，造成事件偵測速度已經提升，但調查、處置與阻斷時間過久，事件可能於調查過程中擴散。

(五)目錄服務、資產管理、防毒系統等中控型主機特權帳號威脅與日

俱增，駭客均以上述特權帳號為竊取與搶奪之標的，因特權帳號持有盤點與管理制度不一，造成風險管控不佳，存取控管管理不易。

二、 計畫目標

（一） 資訊資源向上集中

臺北市進行防毒軟體之集中整合及推動管考機制。

連江縣強化資源向上集中機房之防護及保障資源向上集中後之資訊安全，並加強系統之管理權限，提升機密性防護。

（二） 精進資安防護能量

各縣市政府導入或強化端點偵測及應變機制（EDR），臺北市及花蓮縣持續推動政府機關資安弱點通報機制（VANS），強化弱點管理能量。

三、 計畫內容與實施策略

（一） 臺北市政府

1. 資訊資源向上集中：

(1) 防毒軟體整合：

本府尚有部分機關自行採購防毒軟體，各機關除須投注額外人力與資源進行維運，一線防護資源未有統一標準而整合不易，為加速並標準化資安威脅處置作業，本府統一進行端點安全建置部署，一線端點與二線資安專家 MDR 整合，強化端點安全快速分享與調查之資源整合。

(2) 推動資安管考機制：

本府因前瞻預算之資源，注入了許多資安基礎建設，惟端點、網路之異質資安設備眾多，於端點或網路偵測相關威脅，或有重大情資需請各機關協助處理時，經調查、確認、規劃、隔離、處置、復原等作業需跨平台進行操作，恐因處理時效問題或執行人員資訊不對等而造成資安威脅擴大，降低原有縱深防護之防護密度預期效果。本案引進統一資安管考機制，使各機關統一透過本機制，快速掌握相關資安威脅

與應對處理方式，並藉由統一回報途徑，使本府快速掌握該威脅之處理進度，整體提升資安事件反應速度。

(3) 建置資安與機房維運戰情儀表板：

藉由儀表板來監控各項KPI，如：網站基礎設備、與民眾相關之服務與系統、重要伺服器執行作業之系統容量及網路資源使用率等以自助管理監控即時預警並通知，以確保核心服務可用性。

2. 精進資安防護能量：

(1) 強化端點偵測及應變機制：

持續部署端點偵測及回應程式，以強化防禦外部日新月異的攻擊與趨勢，並引進二線MDR資安情資偵測與處理資安專家團隊，進行主動式大數據分析整合，以持續優化與強化橫向整合分析，整體提升資安事件反應速度。

(2) 推動VANS與資產管理自動整合機制：

將本府資產管理系統與VANS進行整合，以強化電腦軟體弱點管理，加速高風險弱點掌握能力，優先修補高風險弱點，有效強化本府電腦安全。

(二) 金門縣政府

推動本府導入偵測及應變機制(EDR)，佈署端點防護系統，期能於早期發現駭客活動跡象，及早因應處理降低資安風險。

(三) 連江縣政府

1. 本府已進行各單位資訊資源向上集中作業，惟各單位系統大小、功能不一，為強化資源向上集中機房之防護且為保障資源向上集中後集中管理的資訊安全，採購加強機房資安防護之相關設備，如UPS、防火牆等，同時為了增強遭遇災難後的可用性，購買虛擬機及相關設備進行系統備援作業，提升本府系統的可靠性及安全性，並加強資訊資源向上集中機房之系統管理的權限，進入系統或管理界面，須使用雙因子認證機制系統，提升機密性防護。

2. 本縣資安等級B級單位導入端點偵測及應變機制(EDR)，即時監控資安警訊，提升端點防護力。

（四） 花蓮縣政府

為精進地方政府資安防護能量，擬於本府及所屬 B、C 及機關導入資訊系統弱點通報機制(VANS)及端點偵測及應變機制(EDR) 藉由 VANS 及 EDR 的導入提升本府及所屬機關(B、C 級機關)對資安事件的掌握，迅速釐清引發資安事件的來源並有效處理，避免因資安事件的調查費時而導致影響範圍擴散，以彌補 SOC 的不足，詳細導入及續約情形如下：

1. 導入及續約資訊系統弱點通報機制(VANS)：
   預計於本府所屬機關(C 級機關)導入，並於 B 級機關完成續約，以符合中央政策。
2. 導入端點偵測及應變機制(EDR)：
   預計於本府及所屬 B 級機關導入，以符合中央政策。

四、 實施範圍

本計畫實施對象為臺北市政府、金門縣政府、連江縣政府及花蓮縣政府。

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

（一） 臺北市政府

年度	項次	關鍵績效指標	目標值
112	1	防毒軟體整合機關之整合率。 ※公式：(防毒軟體整合之機關數/本府機關數量)*100%	80%
	2	資安管考機制導入機關之導入率。 ※公式：(已導入資安管考機制之機關數/本府機關數量)*100%	100%
	3	核心服務整合至資安與機房維運戰情儀表板之整合率。 ※公式：(本府資訊局已整合至儀表板之核心服務數量/本府資訊局核心服務數量)*100%	70%

113	1	防毒軟體整合機關之整合率。 ※公式：(防毒軟體整合之機關數/本府機關數量)*100%	100%
	2	資安管考機制導入機關之導入率。 ※公式：(已導入資安管考機制之機關數/本府機關數量)*100%	100%
	3	核心服務整合至資安與機房維運戰情儀表板之整合率。 ※公式：(本府資訊局已整合至儀表板之核心服務數量/本府資訊局核心服務數量)*100%	100%

（二） 金門縣政府

年度	項次	關鍵績效指標	目標值
112	1	資通安全責任等級 B 級機關導入 EDR 導入率 (導入 B 級機關個數/B 級機關總數)	100%

（三） 連江縣政府

年度	項次	關鍵績效指標	目標值
112	1	資訊資源向上集中加強防護。 公式：（本府已整合至機房核心系統數量/本府核心系統數量）*100%	100%
	2	符合資通安全責任等級 C 級之本府機關均導入資訊系統弱點通報機制(VANS)。 公式：（B、C 級 VANS 導入數量/B、C 級數量）*100%	100%
	3	符合資通安全責任等級 B 級之本府機關均導入端點偵測及應變機制(EDR)。 公式：（B 級 EDR 導入數量/B 數量)*100%	100%
113	1	資訊資源向上集中備份防護加強。 公式：（本府已整合至機房核心系統備份數量/本府核心系統數量）*100%	100%

（四） 花蓮縣政府

年度	項次	關鍵績效指標	目標值
112	1	符合資通安全責任等級 B、C 級機關之 VANS 導入率公式：(B、C 級導入 VANS 機關數/B、C 級機關總數)*100%	100%

113	1	符合資通安全責任等級B級機關之EDR導入率公式： (B級導入EDR機關數/B級機關總數)*100%	100%

七、 持續營運評估

（一） 臺北市政府

計畫期程結束後，將對相關成果進行效益分析，調整建置範圍，並持續購置相關軟體升級授權(MA)以更新特徵碼或新版軟體，以利後續維護作業。

（二） 金門縣政府

本計畫期程結束後,後續維運方式擬由本府每年度編列預算辦理。

（三） 連江縣政府

資源向上集中相關資安防護設備每年授權費用約 500,000 元，未來將由各單位預算回歸，由本府每年編列相關經費。

（四） 花蓮縣政府

計畫期程結束後，將相關成果進行效益分析並將分析導入資安弱點通報機制針對弱點軟體修復率有無提升進行比較，調整建置範圍,並持續購置相關軟體升級授權(MA)以更新特徵碼或新版軟體,以各機關預算進行後續維護作業。

八、 經費明細概算

（一） 臺北市政府

單位：新臺幣元

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	1. 辦理防毒軟體整合。 2. 推動資安管考機制。 3. 資安與機房維運戰情儀表板。	16,488,505	3,662,500	1. 完成防毒軟體整合機關數達80%。 2. 資安管考機制導入機關數維持100%。 3. 核心服務整合	1

						至資安與機房維運戰情儀表板達 70%。	
	2	精進資安防護能量	1. 持續部署端點偵測及回應程式。 2. VANS 與資產管理自動整合機制持續維運。	6,912,795	0	1. EDR 程式部署機關數達 80%。 2. VANS 與資產管理自動整合，並維持均導入率。	2
小　　計				23,401,300	3,662,500		
合　　計					27,063,800		

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	資訊資源向上集中	1. 辦理防毒軟體整合。 2. 推動資安管考機制。 3. 資安與機房維運戰情儀表板。	16,047,427	4,350,000	1. 完成防毒軟體整合機關數達 100%。 2. 資安管考機制導入機關數維持 100%。 3. 核心服務整合至資安與機房維運戰情儀表板達 100%。	1
	2	精進資安防護能量	1. 持續部署端點偵測及回應程式。 2. VANS 與資產管理自動整合機制持續維運。	67,27,873	0	1. EDR 程式部署機關數達 100%。 2. VANS 與資產管理自動整合，並維持 100%導入率。	2
小　　計				22,775,300	4,350,000		

合　　計	27,125,300		

（二） 金門縣政府

單位：新臺幣元

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	導入端點偵測及應變機制(EDR)	推動本府包含所屬3個資安責任等級B級機關約1200臺主機導入EDR。	0	6,000,000	導入EDR至3個B級機關。	1
小　　計				0	6,000,000		
合　　計					6,000,000		

（三） 連江縣政府

單位：新臺幣元

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	資源向上集中之資安防護。	2,200,000	2,325,000	資源向上集中之資安防護設備加強	1
	2	精進資安防護能量	建置連江縣政府B級各機關端點偵測及應變機制(EDR)及C級機關VANS。	1,224,000	0	B級MDR及C級VANS完成導入	2
小　　計				3,424,000	2,325,000		
合　　計					5,749,000		

年度	項次	工作	工作內容	所需經費	績效	優

		項目		經常門	資本門	目標	先次序
113	1	資訊資源向上集中	資源向上集中之資安防護。	2,750,611	2,170,000	資源向上集中之資安防護設備加強。	1
小　　計				2,750,611	2,170,000		
合　　計				4,920,611			

（四） 花蓮縣政府

單位：新臺幣元

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	落實資安縱深。	建置縣政府及所屬機關(B、C級機關)之資安弱點通報系統(VANS)，預計導入的電腦數約為4,672。	3,572,000	0	導入VANS	1
	2	落實端點偵測。	建置縣政府及所屬機關(B級機關)之端點偵測及應變機制(EDR)，預計導入的電腦數約為2,460。	10,716,000	0	導入EDR	2
小　　計				14,288,000	0		
合　　計				14,288,000			

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年	1	落實端點偵測。	建置縣政府及所屬機關(B級機關)之端點偵測及應變機制(EDR)，預計導入的電腦數約為2,460。	13,422,667	0	導入EDR。	1
小　　計				13,422,667	0		
合　　計				13,422,667			

九、 經費補助表

（一） 臺北市政府

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	27,063,800	0	13,531,900	13,531,900
113年	27,125,300	0	13,562,650	13,562,650

（二） 金門縣政府

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	6,000,000	0	1,800,000	4,200,000

（三） 連江縣政府

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	5,749,000	0	574,900	5,174,100
113年	4,920,611	0	492,061	4,428,550

（四） 花蓮縣政府

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	14,288,000	0	1,428,800	12,859,200
113 年	13,422,667	0	1,342,267	12,080,400

十、 預定進度

（一） 臺北市政府

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
112/5	約 43%	11,637,434	資訊安全服務月報或相關報告。
112/11	約 79%	21,380,402	資訊安全服務月報或相關報告。
113/1	100%	27,063,800	1. 資訊安全服務月報或相關報告。 2. 實際將於隔年 1 月份完成查核（查驗或驗收），故於隔年 1 月份關帳前完成付款及申請作業。

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
113/5	約 42%	11,392,626	資訊安全服務月報或相關報告。
113/11	約 80%	21,700,240	資訊安全服務月報或相關報告。
114/1	100%	27,125,300	1. 資訊安全服務月報或相關報告。 2. 實際將於隔年 1 月份完成查核（查驗或驗收），故於隔年 1 月份關帳前完成付款及申請作業。

（二） 金門縣政府

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
112/4	30%	1,800,000	採購 EDR

112/10	100%	6,000,000	EDR 驗收、付款

（三） 連江縣政府

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
112/6	約 21%	1,224,000	完成 2 個 B 級機關 MDR 及 C 級機關 VANS 導入
112/11	100%	5,749,000	完成資源向上集中資安防護設備加強

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
113/6	約 56%	2,750,611	完成資源向上集中資安防護設備加強
113/12	100%	4,920,611	完成資源向上集中資安防護設備加強

（四） 花蓮縣政府

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
112/6	30%	4,286,400	1. VANS 之購置作業，以及通知協調 B、C 級機關辦理 VANS 導入或續約之先期作業。 2. EDR 之購置作業，以及通知協調 B 級機關辦理 EDR 導入之先期作業。
112/12	100%	14,288,000	VANS、EDR 導入、續約及驗收完成。

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
113/6	30%	4,026,800	EDR 之購置作業，以及通知協調 B 級機關辦理 EDR 續約之先期作業。
113/12	100%	13,422,667	EDR 續約及驗收完成。

十一、 預期效益

（一） 臺北市政府

1. 資訊資源向上集中：

(1) 防毒軟體整合：

統合防毒軟體資源，統一進行端點安全建置部署，強化端點安全快速分享與調查之資源整合。

(2) 推動資安管考機制：

引進統一資安管考機制，快速掌握相關資安威脅與應對處理方式，並藉由統一回報途徑，使本府快速掌握該威脅之處理進度，整體提升資安事件反應速度。

(3) 建置資安與機房維運戰情儀表板：

藉由儀表板即時監控各項 KPI，自助管理監控即時預警並通知，以確保核心服務可用性。

2. 精進資安防護能量：

(1) 強化端點偵測及應變機制：

強化端點防護架構，並透過 MDR 提高跨平台異質資安防護設備大數據分析能力，提高應變能量。

(2) 推動 VANS 與資產管理自動整合機制：

提高本府電腦弱點可視性，快速鎖定應修補之風險之處。

(二) 金門縣政府

佈署端點威脅防禦系統，採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，以利加速採證及資安鑑識作業。

(三) 連江縣政府

1. 本府已進行各單位資訊資源向上集中作業，惟各單位系統大小、功能不一，為強化資源向上集中機房之防護，採購相關資安防護軟硬體設備，提升資安防護，同時機房虛擬化，以雲端方式進行系統備份或備援作業，降低被攻擊的可能性及事件發生後的衝擊性；且加強資訊資源向上集中機房之系統管理的權限，進入系統或管理界面，須使用雙因子認證機制系統，提升機密性防護。
2. 建置連江縣政府 B 級各機關端點偵測及應變機制(EDR)，及 C 級機關 VANS 導入。

（四） 花蓮縣政府

1. VANS 導入

（1）推動 VANS 與資產管理自動整合機制，強化弱點管理能量，提高電腦風險可視性。

（2）VANS 能呈現導入設備資訊資產的版本與漏洞資訊，對一定風險程度以上之漏洞能主動通報，能縮短調查時間並減少零時差攻擊的風險。

2. EDR 導入

（1）推動 EDR 機制，強化偵測端點系統上異常活動，降低資安風險。

（2）EDR 能主動監控端點，針對具有威脅跡象的活動蒐集資料，並對其分析，識別是否有任何已知的威脅，以自動化降低人工識別風險的時間。

十二、相關聯絡資料

機關單位	姓名	電話	E-mail
臺北市政府	李政諺	02-27208889 #51518	Security@gov.taipei
臺北市政府	吳思瑩	02-27208889 #51511	
金門縣政府	劉家銘	082-318823 #62959	Ming734105@mail.kinmen.gov.tw
連江縣政府	丁燕妮	0836-25139 #6563	matsumis33@outlook.com
花蓮縣政府	洪維澤	03-8234756 #328	kaede@hl.gov.tw

附件2

政府基層機關資安主動防禦之分項計畫

新北市政府(含基隆市、宜蘭縣政府)

計畫全程：112年1月至113年12月

政府基層機關資安主動防禦計畫

一、 計畫緣起

資通安全管理法於110年8月23日修法通過，依據資通安全責任等級分級辦法規定，須持續落實執行「管理面」、「技術面」及「認知與教育訓練」等法遵事項，為配合行政院辦理112年至113年前瞻基礎建設-政府基層機關資安主動防禦計畫」，以「資訊資源向上集中」、「精進政府基層機關資安防護能量」及「推動滲透測試及紅藍軍攻防演練」為三大計畫目標，據以推動服務、系統及網站統合集中至共用資料中心，全面導入資安弱點通報機制及部署端點防護機制，強化基層機關資安防護能量，並持續發展滲透測試與紅藍隊演練，以改善機關資安防護及培育國內資安人才，特擬訂本計畫。

二、 計畫目標

（一） 資訊資源向上集中

1. 規劃將新北市政府所屬機關之自管資通系統以虛擬化方式向上集中整合至市府機房，並完成虛擬化資源擴充與備份與備援資料中心建置、網路頻寬提升及資安防禦設備汰換等，提高系統可用性與穩定性，以達到資料中心減量、老舊伺服器汰除及降低資安風險。
2. 整併新北市政府所屬機關自行建置之AD目錄服務系統，集中化管理各系統服務與資通訊設備身分驗證識別，以達到多項整併效益，包括政府組態基準GCB部署、資安弱點通報機制導入及強化資安監控等。
3. 提升共用資料中心能量，持續推動基隆市政府所屬機關、單位資訊資源向上集中，包含擴充效能不足之虛擬主機平台、優化網路基礎建設及骨幹網路連線品質及汰換效能不足之防火牆。
4. 宜蘭縣政府將重點強化網路整併與資訊資源向上集中，包含資訊共用機房設備建置、共用資料中心建置、電子郵件資訊安全防護系統建置及電路向上集中。

（二） 精進資安防護能量

1. 推動新北市政府、基隆市政府及宜蘭縣政府共 18 個 B 級機關導入端點偵測及應變機制(EDR)，並依資通安全管理法規定提交端點偵測及應變機制偵測資料，總計導入總數約 1 萬 3,690 個設備。
2. 推動新北市政府、基隆市政府及宜蘭縣政府共 65 個 C 級機關導入資安弱點通報機制(VANS)，總計導入總數約 1 萬 3,020 個設備。
3. 宜蘭縣政府與異地端中興文創智慧聯網共用中心，所共用之交換器介面不足，府本部主機房骨幹交換器介面亦不足，為能落實資安防禦縱深及提高資料可用性，抵禦因疫情或複合性天然災害的衝擊，異地端可規劃作為臨時辦公處所，故需要佈設網路安全防護設備，另建置分析網路速率系統及負載平衡設備，提升網路的可用性及服務品質。

（三） 推動滲透測試及紅藍軍攻防演練

新北市、基隆市及宜蘭縣辦理紅藍軍資安攻防演練及滲透測試專案，厚實資安防護能量，培植機關資安人才，每年培訓至少 23 人次。

三、 計畫內容與實施策略

（一） 資訊資源向上集中

1. 新北市政府既有雲端虛擬化環境平台已提供所屬機關共同使用達 700 臺以上虛擬主機，架設市府大型服務網站，包含各機關官網、疫苗預約網站及市民雲等，朝單一資料中心為目標縮減所屬機關主機數量，除可集中化管理外，亦可汰除老舊伺服器，降低資安風險，因系統使用效能已屆 70%以上，為滿足資訊資源向上集中需求，規劃擴充雲端虛擬化環境平台資源。
2. 新北市政府共 489 個公務機關，各機關所建資通系統及網站眾多，但各系統網站之備份機制均不相同，有使用資訊中心備份系統、有自行安裝備份軟體或委由廠商協助備份等方式，且異地備援機制亦不完善或欠缺，其中 C 級機關更顯匱乏，當發生嚴重異常事件時，恐發生無法復原或復原速度過慢的問題，為

達成資訊資源向上集中，整合由資訊中心統一管理與制訂完善備份模式，本府規劃建置集中化備份與備援資料中心，重新規劃部建資訊中心機房及台中異地備援機房，評估全府各機關所需備份與備援資源，全數納入集中化管理，提高備份與備援效率且確保備份機制有效運作。

3. 新北市政府經行政院核定之資通安全責任等級 B 級機關共有 11 個，C 級機關共有 48 個，其中現行資料中心除資訊中心外，尚有警政、財稅、戶政、地政及教網等專線機房，以及部分 C 級機關仍有維運自行或委外設置、開發之資通系統，規劃將資安責任等級 B 級及部分 C 級機關(例如：板橋區公所、新莊區公所、樹林區公所、永和區公所等)之自管資通系統(例如：AD 目錄服務系統)以虛擬化方式向上集中整合至市府機房，因本府行政網路環境已高度完成整併，既有線路頻寬已不敷使用，為避免向上集中整合後造成網路擁塞及提高服務運作穩定性，規劃提升市府出口網路及 GSN VPN 線路頻寬，並建置網路負載平衡機制。

4. 為滿足新北市政府資訊資源向上集中後之資安防護需求，亟需規劃汰換及擴充多項資安防禦設備如下：

(1) 出口閘道端之入侵偵測防禦系統(IPS)已使用長達 6 年且效能負載過高，時常發生當機或檢查效率不佳，規劃汰換全新入侵偵測防禦系統，強化網路封包檢查，提供全府 2 萬餘公務同仁電腦及伺服器安全性防護。

(2) 既有 2 座網頁應用程式防火牆(WAF)已收整數百個服務網站，並針對各網站增加 irule 防護檢查規則，已無法再容納市府對外服務網站，為避免產生資安漏洞，亟需增建網頁應用程式防火牆(WAF)擴大收整本府所屬 B、C 級機關資通訊系統。

(3) 本府雖已統籌辦理 B 級機關資安威脅偵測監控(SOC)，惟現有儲存空間僅有 150TB 且資料收集器則僅有 11 臺，然而 B 級機關之核心資通訊系統眾多且部分機關採實體內外網隔離(例如：地政局、警察局、稅捐稽徵處等)，以及 C 級機關亦

有許多自管資通訊系統，儲存設備及資料收集器之數量與空間均無法負荷，為全面落實資安威脅偵測監控，亟須擴充資安日誌系統(NetProxy)以提升日誌儲存效率及儲存範圍，確保資安監控完整並提升資安事件處理效率。

5. 整併新北市政府所屬機關自行建置之 AD 目錄服務系統，本府行政網路環境雖已高度完成整併，惟早期為因應所屬機關業務特性，有部分機關及區公所仍維持自建自管 AD 目錄服務系統，增加市府整體資安管理及監控負擔，爰規劃向上集中整合管理，統一各系統服務與資通訊設備身分驗證識別，以達多項整合效益，包括提升政府組態基準 GCB 部署效率、資安弱點通報機制導入及強化資安監控等。
6. 提升基隆市政府資訊機房服務能量，轉型為基隆市共用資料中心擴充效能不足之虛擬主機平台，改善整體 CPU 及記憶體資源不足，使用量經常超出平均 60%以上，因目前虛擬主機已收納超過 120 台實體伺服器，考量逐年納入各機關、單位資通系統，需提升設備運作之穩定性。
7. 優化基隆市政府網路基礎建設及骨幹網路連線品質，建置高可用性網路負載平衡，優化市府對外線路頻寬，提升可用性（HA）及即時備援切換能力，以因應線路整併新增需求。
8. 汰換基隆市政府效能不足之防火牆，以滿足資料中心資安防護效能需求。
9. 宜蘭縣政府現有主機房有府本部二樓主機房及三樓戶、役、地政機房兩處外，在 108 年獲內政部建築研究所永續智慧社區創新實證示範計畫補助案於五結中興文創園區建置慧聯網共用中心，與本府以租用之光纖連接，初具溪南、溪北互為備份機房的功能，府內約有 260 餘部伺服主機、90 餘部網路設備及 57 座資訊機櫃，規劃辦理本府二樓機房消防建置、資訊及網路設備機櫃汰換、機櫃式空調系統設備換裝、機櫃式不斷電系統建置、機櫃式智慧型精密配電櫃裝設、智慧多功能數位電表建置、環控系統更新、光纖及網路通信環境鋪設及相關裝修工程等，與中興文創園區建置智慧聯網共用中心機房進行相互備

援，確保資料安全，配合虛擬化作業之資料共用中心系統建設進行集中管理，以達資訊設備減量及效能提升，提升公務運作效率。

10. 建置宜蘭縣政府共用資料中心，於本府虛擬化平台上建構超融合設備，主要系統設備建置於縣府主機房，異地備援系統設備建置於中興文創智慧聯網共用中心，將分年建置共用資料中心虛擬化平台設備5台及備援中心虛擬化平台設備5台共計10台，相關軟體、備份儲存設備、虛擬化平台之防毒、虛擬化平台資安系統及維運與稽核管理功能之建立，提供自動化部署服務，打造彈性靈活的架構環境。

11. 宜蘭縣政府入口網(EIP)及共用資料庫目前為集中共構之系統，供縣轄所屬機關使用，因導入服務及使用者與日俱增，擬進行硬體升級以確保系統集中共用之效能可靠及穩定性，預計推動6個機關(衛生局、消防局、環境保護局、文化局、縣史館、蘇澳鎮公所)行政業務服務導入服務。

12. 宜蘭縣政府電子郵件系統為104年建置，系統版本老舊且資安防護規劃缺乏，僅有基本惡意郵件防治模組，將規劃建置共通性電子郵件核心系統，透過單主機多網域管理，完整管控郵件收發權限，達成弱密碼分析、OTP 防護、異地登入警示，引導式分類管理主控台，多重條件的郵件分類過濾等，達到電子郵件稽核及過濾相關資訊安全防護，統一進行安全性控管，預計可整合186個所屬機關單位，使用人數約1萬2,000人。

13. 宜蘭縣政府自91年起即開始進行線路整併納入GSN作業，歷經多年，雖然在共用系統如全縣性公文管理系統、公文電子交換系統、員工業入口務網、電子郵件服務及資訊安全防護等作業等較易於統整推動，但因為縣府對外網際網路及對內伺服器區共用服務的頻寬提供，隨著業務的集中與資安監控業務的持續推動，仍時常有尖峰時刻總頻寬不足的情形發生，總計目前資安機關除學校係使用學術網路並與本府有電路串接外，全縣121個資安機關計有105個機關已完成GSN/VPN線路整併，因應資安法實施，鼓勵並統整縣內仍未加入GSN/VPN的資安機關

加入宜蘭縣之整合 VPN，除學校使用學術網路(TANet)外，目前尚有 22 個資安機關尚未納入，本項目預計至少將 10 個資安機關納入服務，以強化全縣資安防護網之完整性。

（二） 精進資安防護能量

1. 依資通安全管理法遵事項，推動新北市政府、基隆市政府及宜蘭縣政府共 18 個 B 級機關導入端點偵測及應變機制(EDR)，並提交端點偵測及應變機制偵測資料，總計導入總數約 1 萬 3,690 個設備(新北市 9,500 個、基隆市 2,190 個、宜蘭縣 2,000 個)。
2. 依資通安全管理法遵事項，推動新北市政府、基隆市政府及宜蘭縣政府共 65 個 C 級機關導入資安弱點通報機制(VANS)，總計導入總數約 1 萬 3,020 個設備(新北市 11,000 個、基隆市 900 個、宜蘭縣 1,120 個)。
3. 宜蘭縣政府與異地端中興文創智慧聯網共用中心，所共用之交換器介面不足，府本部主機房骨幹交換器介面亦不足，為能落實資安防禦縱深及提高資料可用性，抵禦因疫情或複合性天然災害的衝擊，異地端可規劃作為臨時辦公處所，故需要佈設網路安全防護設備，另建置分析網路速率系統及負載平衡設備，提升網路的可用性及服務品質。

（三） 推動滲透測試及紅藍軍攻防演練

規劃辦理方式及預計成效說明如下：

1. 新北市政府：辦理紅藍軍資安攻防演練及滲透測試專案，透過紅、藍隊分組攻防演練及滲透測試方式，檢視機關整體資安防護措施，進而找出問題及改善策略，並訓練內部人員事件處理應變能力，培植機關資安人才，每年培訓人才至少 10 人次。
2. 基隆市政府：針對資安事件蒐集相關資訊，將駭客所植入的惡意程式檔案，進行逆向工程分析。再將此案例及經驗納入後續資安人才培訓課程，增強人才實證場域經驗。

(1) 紅藍隊培訓培訓 6 人次以上(每年 3 人次)，項目如下：

A. 提供如何取得客戶機敏資訊演練及培訓(紅隊)。

B. 提供如何取得具有中控性質之主機（如 AD、防毒系統）演練及培訓(紅隊)。

C. 提供系統防護及內網為些通報應變演練及培訓(藍隊)。

D. 惡意程式偵測、分析演練及培訓(藍隊)。

E. EDR 逆向工程演練演練及培訓(藍隊)。

F. 網路封包分析演練及培訓(藍隊)。

(2) 紅藍隊模擬對抗演練 2 場次以上(每年 1 場次)。

(3) 輔導培訓機關資安人員取得資通安全專業證照清單之技術類證照共 1 張以上。

3. 宜蘭縣政府：培訓本縣機關內部人員、本縣系統開發及維護有關之廠商系統人員、軟體工程師、資安相關科系學生，每年培訓人才至少 10 人次，完成培訓之人力可規劃後續參與本縣之紅藍攻防演練，強化本縣資安防護能力。

四、 實施範圍

本計畫實施對象為新北市政府、基隆市政府及宜蘭縣政府。

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

（一） 新北市政府

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	1
	2	完成本府所屬機關自行建置之 AD 目錄服務系統整併(整併機關數/自行建置機關數)	100%
	3	資通安全責任等級 C 級機關導入介接 VANS 導入率(導入 C 級機關個數/C 級機關總數，C 級機關總數 48 個)	100%
	4	資通安全責任等級 B 級機關導入 EDR 導入率(導入 B 級機關個數/B 級機關總數，B 級機關總數 11 個)	100%
	5	提供公務網路環境場域，辦理資安紅藍軍攻防演練及滲透測試，培訓至少 10 人次	10
113	1	完成資料中心減量個數	1
	2	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率(導入 B 級機關個數/B 級機關總數，B 級機關總數 11 個)	100%
	3	提供公務網路環境場域，辦理資安紅藍軍攻防演練及滲透測試，培訓至少 10 人次	10

（二） 基隆市政府

年度	項次	關鍵績效指標	目標值
112	1	維持虛擬平台 CPU 與記憶體資源使用率	50%
	2	提升資料中心之對外總網路頻寬（Gbps）	2
	3	提升資料中心防火牆 throughput(Gbps)	5
	4	資通安全責任等級 C 級機關導入介接 VANS 導入率(導入 C 級機關個數/C 級機關總數，C 級機關總數 7 個)	100%
	5	資通安全責任等級 B 級機關導入 EDR 導入率(導入 B 級機關個數/B 級機關總數，B 級機關總數 4 個)	100%
	6	資安實戰培訓人才（人次）	3
	7	攻防演練實證場域或資安檢測（場次）	1
113	1	維持虛擬平台 CPU 與記憶體資源使用率	50%
	2	資通安全責任等級 B 級機關導入 EDR 導入率(導入 B 級機	100%

		關個數/B 級機關總數，B 級機關總數 4 個）	
	3	資安實戰培訓人才（人次）	3
	4	攻防演練實證場域或資安檢測（場次）	1

（三） 宜蘭縣政府

年度	項次	關鍵績效指標	目標值
112	1	完成資訊共用機房設備建置，整併減少電腦機房機櫃數 15 組	15
	2	完成 3 個所屬機關之行政業務服務導入共用資料中心	3
	3	完成電子郵件安全防護系統建置，整合提供所屬 186 個機關學校使用	186
	4	完成 10 個所屬機關線路整併	10
	5	完成大型交換器 2 台與小型交換器 6 台汰換，及分析網路速率系統建置	8
	6	資通安全責任等級 C 級機關導入介接 VANS 導入率(導入 C 級機關個數/C 級機關總數，C 級機關總數 10 個)	100%
	7	資通安全責任等級 B 級機關導入 EDR 導入率(導入 B 級機關個數/B 級機關總數，B 級機關總數 3 個)	100%
	8	提供公務網路環境場域，辦理資安紅藍軍攻防演練及資安檢測，培訓至少 10 人次	10
113	1	完成 3 個所屬機關之行政業務服務導入共用資料中心	3
	2	完成大型交換器 2 台汰換	2
	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率(導入 B 級機關個數/B 級機關總數，B 級機關總數 3 個)	100%
	4	提供公務網路環境場域，辦理資安紅藍軍攻防演練及資安檢測，培訓至少 10 人次	10

七、 持續營運評估

本計畫以資訊資源向上集中為目標，將可大幅降低機關資訊經費與人力負擔，計畫完成後相關硬體設備及服務項目之永續經營模式，除持續編列公務預算支應外，將積極爭取其他預算，或採取統合資源方式有效運用經費，例如新北市政府依市議會決議統籌辦理各項資通安全管理法應辦事項，以撙節經費及發揮綜效。

八、 經費明細概算

（一） 新北市政府

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	擴充雲端虛擬化環境平台資源。	2,500,000	17,000,000	完成 1 個資料中心減量。	1
			建置備份與備援資料中心。	0	5,000,000		2
			汰換及擴充市府多項資安防禦設備。	3,500,000	15,000,000		3
	2	精進資安防護能量	推動 C 級機關導入資安弱點通報機制。	5,000,000	18,000,000	資通安全責任等級 C 級機關導入介接 VANS 導入率 100%。	4
	3	推動滲透測試及紅藍軍攻防演練	辦理資安紅藍軍攻防演練及滲透測試。	2,000,000	0	提供公務網路環境場域，辦理資安紅藍軍攻防演練及滲透測試，培訓至少 10 人次。	5
小　　計				13,000,000	55,000,000		
合　　計				68,000,000			

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	資訊資源向上集中	擴充雲端虛擬化環境平台資源。	20,000,000	0	1. 完成1個資料中心減量。	2
			建置備份與備援資料中心。	1,200,000	19,342,000	2. 完成本府所屬機關自行	3

			提升市府出口網路及GSN VPN線路頻寬,並建置網路負載平衡機制。	17,114,000	0	建置之AD目錄服務系統整併。	1
			汰換及擴充市府多項資安防禦設備。	5,000,000	25,000,000		4
			整併本府所屬機關自行建置之AD目錄服務系統。	5,000,000	0		5
	2	推動滲透測試及紅藍軍攻防演練	辦理資安紅藍軍攻防演練及滲透測試。	2,000,000	0	提供公務網路環境場域，辦理資安紅藍軍攻防演練及滲透測試，培訓至少10人次。	6
小　　計				50,314,000	44,342,000		
合　　計					94,656,000		

（二） 基隆市政府

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	虛擬平台升級擴充。	0	2,500,000	因應系統集中化，擴增伺服器、記憶體、儲存空間及虛擬平台作業系統軟體，提升整體設備運作之穩定性，維持虛擬平台CPU與記憶體資源使用率50%。	3
			提升資料中心之對外網路優化升級及備援方案。	0	2,500,000	建置高可用性網路負載平衡，優化市府對外	1

						線路頻寬，提升可用性(HA)及即時備援切換能力，以因應線路整併新增需求，提升資料中心之對外總網路頻寬2GB。	
			資料中心防火牆效能升級方案。	0	2,500,000	因應系統集中化，汰換效能不足之防火牆，以滿足資料中心資安防護效能需求，提升資料中心防火牆throughput 5GB。	2
	2	精進資安防護能量	推動C級機關導入資安弱點通報機制。	0	1,400,000	資通安全責任等級C級機關導入介接VANS導入率達100%。	2
			推動B級機關導入端點偵測及應變機制。	0	2,000,000	資通安全責任等級B級機關導入EDR導入率達25%。	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檢測,協助地方政府改善資安防護。與國內產業合作,訓練紅藍隊資安攻防人才。	2,000,000	0	辦理紅藍軍攻防模擬演練或資安主動式檢測1案次，透過相關教育訓練及桌面模擬推演，提升參演人員事件處理應變能力，與業界共同訓練紅藍隊資安攻防人員至少3人次。	2
小　　計				2,000,000	10,900,000		
合　　計					12,900,000		

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	資訊資源向上集中	虛擬平台升級擴充。	0	4,500,000	因應系統集中化,擴增伺服器、記憶體、儲存空間及虛擬平台作業系統軟體，提升整理設備運作之穩定性，維持虛擬平台 CPU 與記憶體資源使用率 50%。	3
	2	精進資安防護能量	推動 B 級機關導入端點偵測及應變機制。	0	2,000,000	資通安全責任等級 B 級機關導入 EDR 導入率達 100%。	1
	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檢測，協助地方政府改善資安防護。與國內產業合作，培訓紅藍隊資安攻防人才。	3,000,000	0	辦理紅藍軍攻防演練或資安主動式檢測 1 案次，透過相關教育訓練及於桌面或實地環境攻防演練，提升參演人員事件處理應變能力，與業界共同訓練紅藍隊資安攻防人員至少 3 人次,2 年累計共計 6 人次。	2
小　　計				3,000,000	6,500,000		
合　　計					9,500,000		

（三） 宜蘭縣政府

年度	項次	工作項目	工作內容	所需經費		績效目標	優先次
				經常門	資本門		

							序
112	1	資訊資源向上集中	資料共用中心擴充- 1.購置 3 台共用資料中心虛擬化平台設備及資安、申請機制相關。 2.軟體購置 2 台共用資料中心中階虛擬化平台設備及相關軟體。 3.建置 1 台共用資料中心虛擬化平台備份儲存設備(60TB)。	0	4,160,000	推動 3 個機關行政業務服務導入本共用資料中心提供服務。	5
			電子郵件安全防護系統建置- 1.電子郵件系統。 2.郵件過濾系統。 3.郵件社交工程防護解決方案。 4.郵件 APT 防禦解決方案。 5.郵件 BEC 可疑信件防禦解決方案。 6.郵件稽核系統。	0	8,868,000	完成本縣 186 個機關學校使用。	6
			電路向上集中-集中整併 10 個機關納入本府內部網路(GSNVPN)	120,000	950,000	集中整併 10 個機關納入本府內部網路(GSNVPN)。	4
	2	精進資安防護能量	骨幹網路安全防護- 1.汰換大型交換器。 2.汰換小型交換器。 3.建置分析網路	0	8,440,000	1.汰換大型交換器 2 台。 2.汰換小型交換器 6 台。 3.建置分析網路速率系統。	7

			速率系統				
			推動C級機關導入資安弱點通報機制。	3,360,000	0	資通安全責任等級C級機關導入介接VANS導入率100%。	1
			推動B級機關導入端點偵測及應變機制。	7,000,000	0	資通安全責任等級B級機關導入EDR導入率100%。	2
	3	推動滲透測試及紅藍軍攻防演練	培訓資安人才至少10人次，辦理紅藍軍資安攻防演練及滲透測試	980,000	0	每年培訓資安人才至少10人次，辦理紅藍軍資安攻防演練及滲透測試	3
小　　計				11,460,000	22,418,000		
合　　計					33,878,000		

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	資訊資源向上集中	資訊共用機房設備建置- 1.消防建置 2.機房區資訊及網路設備機櫃 3.機房區機櫃式空調系統設備 4.機房區機櫃式不斷電系統組 5.機房區機櫃式智慧型精密配電櫃 6.智慧多功能數位電表 7.環境及圖形控制系統	0	12,300,000	現有2樓電腦機房機櫃數由原有30組傳統機櫃減少至15組。	5

			8.基礎光纖及網路通信環境鋪設及建置 9.裝修工程				
			資料共用中心擴充- 1.購置1台共用資料中心虛擬化平台設備及資安、申請機制相關 2.建置5台異地備援系統虛擬化平台設備及相關軟體	4,045,000	28,500,000	推動3個機關行政業務服務導入本共用資料中心提供服務。	3
	2	精進資安防護能量	骨幹網路安全防護-汰換大型交換器	0	1,600,000	汰換大型交換器2台	4
			推動B級機關導入端點偵測及應變機制	7,000,000	0	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率100%。	1
	3	推動滲透測試及紅藍軍攻防演練	培訓資安人才至少10人次並辦理紅藍軍資安攻防演練及滲透測試	980,000	0	每年培訓資安人才至少10人次，辦理紅藍軍資安攻防演練及滲透測試	2
小　　計				12,025,000	42,400,000		
合　　計					54,425,000		

九、 經費補助表

（一） 新北市政府

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	68,000,000	0	27,200,000	40,800,000
113年	94,656,000	0	37,863,000	56,793,000

本府計畫補助經費比率為 60%，113 年行政院補助款為 56,793,000 元(經常門 30,188,000 元、資本門 26,605,000 元)，因預算編列使用千元為單位，本府自籌款編列 37,863,000 元(經常門 20,126,000 元、資本門 17,737,000 元)。

（二） 基隆市政府

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	12,900,000	0	2,580,000	10,320,000
113 年	9,500,000	0	1,900,000	7,600,000

（三） 宜蘭縣政府

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	33,878,000	0	6,776,000	27,102,000
113 年	54,425,000	0	10,885,000	43,540,000

1. 本縣計畫補助經費比率為 80%，112 年行政院補助款為計畫總金額為 27,102,000 元(經常門為 9,168,000 元、資本門為 17,934,000 元)，本府自籌款為 6,776,000 元(經常門為 2,292,000 元、資本門為 4,484,000 元)。
2. 因行政院 112 年資本門補助款為 17,934,000 元，依規定本縣配合款比率 20%計算結果為 4,483,500 元，考量預算編列使用千元為單位，本縣資本門配合款規畫為 4,484,000 元。

十、 預定進度

（一） 新北市政府

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
112	100%	68,000,000	1. 完成 1 個資料中心減量。 2. 資通安全責任等級 C 級機關導入介接 VANS 導入率 100%。 3. 資通安全責任等級 B 級機關導入 EDR 導入率 100%。

			4. 完成紅藍軍資安攻防演練及滲透測試，提交成果報告書。

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
113	100%	94,656,000	1. 完成1個資料中心減量。 2. 完成本府所屬機關自行建置之 AD 目錄服務系統整併。 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率100%。 4. 完成紅藍軍資安攻防演練及滲透測試，提交成果報告書。

（二） 基隆市政府

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
112	100%	12,900,000	1. 維持虛擬平台 CPU 與記憶體資源使用率50%。 2. 提升資料中心之對外總網路頻寬2GB。 3. 提升資料中心防火牆 throughput 5GB。 4. 資通安全責任等級 C 級機關導入介接 VANS 導入率達100%。 5. 資通安全責任等級B級機關導入EDR導入率達25%。 6. 資安實戰培訓人才3人次。 7. 攻防演練實證場域或資安檢測1場次。

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
113	100%	9,500,000	1. 維持虛擬平台 CPU 與記憶體資源使用率50%。 2. 資通安全責任等級B級機關導入EDR導入率達100%。 3. 資安實戰培訓人才3人次。 4. 攻防演練實證場域或資安檢測1場次。

（三） 宜蘭縣政府

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
112	100%	33,878,000	1. 推動3個機關行政業務服務導入本共用資料中心提供服務。 2. 整併全縣186個機關單位電子郵件資訊安全防護暨過濾系統升級。 3. 集中整併 10 個機關納入本府內部網路(GSNVPN)。 4. 骨幹網路安全防護，汰換大型交換器2台、汰換小型交換器6台及建置分析網路速率系統。 5. 持續辦理本縣機關資訊系統的安全防禦縱深，推動本縣所有 C 級機關共 10 個，導入資訊系統弱點通報機制(VANS)。 6. 辦理本縣機關資訊系統的安全防禦縱深，持續推動本縣所有B級機關共3個，導入端點偵測及應變機制(EDR)。 7. 培訓資安人才至少 10 人次並完成紅藍攻防演練與滲透測試。

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
113	100%	42,125,000	1. 完成資訊共用機房設備建置，整併現有現有2 樓電腦機房機櫃數由原有 30 組傳統機櫃減少至15組。 2. 推動3個機關行政業務服務導入本共用資料中心提供服務。 3. 骨幹網路安全防護，汰換大型交換器2台。 4. 辦理本縣機關資訊系統的安全防禦縱深，持續推動本縣所有B級機關共3個，導入端點偵測及應變機制(EDR)。 5. 培訓資安人才至少 10 人次並完成紅藍攻防演練與滲透測試。

十一、 預期效益

（一） 新北市政府

1. 完成資安責任等級B級及部分C級機關之自管資通系統以虛擬化方式向上集中整合至市府機房，並完成虛擬化資源擴充與備份與備援資料中心建置、網路頻寬提升及資安防禦設備汰換整合等，以達資料中心減量之目標。
2. 完成所屬機關自行建置之AD目錄服務系統整併，集中化管理各系統服務與資通訊設備身分驗證識別，以達到多項整併效益，包括有利於政府組態基準GCB部署、資安弱點通報機制導入及強化資安監控等。
3. 依資通安全管理法遵事項，完成11個B級機關導入端點偵測及應變機制，並提交端點偵測及應變機制偵測資料。
4. 依資通安全管理法遵事項，完成48個C級機關導入資安弱點通報機制。
5. 辦理紅藍軍資安攻防演練及滲透測試專案，透過紅、藍隊分組攻防演練及滲透測試方式，檢視機關整體資安防護措施，進而找出問題及改善策略，並訓練內部人員事件處理應變能力，培植機關資安人才。

（二） 基隆市政府

1. 完成虛擬平台升級擴充，逐年提升整體設備及效能運作之穩定性並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。
2. 提升資料中心之對外網路優化升級及備援方案，建置高可用性網路負載平衡，優化市府對外線路頻寬，提升可用性(HA)及即時備援切換能力，以因應線路整併新增需求。
3. 依資通安全管理法遵事項，完成4個B級機關導入端點偵測及應變機制，佈署端點威脅防禦系統，採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，以利加速採證及資安鑑識作業。
4. 依資通安全管理法遵事項，完成7個C級機關導入資安弱點通

報機制。

5. 針對資安事件蒐集相關資訊，將駭客所植入的惡意程式檔案，進行逆向工程分析。再將此案例及經驗納入後續資安人才培訓課程，增強人才的實證場域經驗。

（三） 宜蘭縣政府

1. 完成資訊共用機房設備建置，整併現有 2 樓電腦機房機櫃數由原有 30 組傳統機櫃減少至 15 組。
2. 建置共用資料中心虛擬化平台設備 5 台及備援中心虛擬化平台設備 5 台及相關軟體、備份儲存設備、虛擬化平台之防毒、虛擬化平台資安系統及維運與稽核管理功能之建立，至少整併 6 個機關導入提供自動化部署服務，打造彈性靈活的架構環境。
3. 整併所屬 186 個機關單位電子郵件資訊安全防護暨過濾系統升級，重新規劃建置安全穩定高效能之共通性電子郵件核心系統，升級郵件資安防護，增加社交工程、郵件稽核、郵件詐騙防護機制、阻攔 APT 攻擊功能。
4. 網路整併升級及負載平衡設備，統整宜蘭縣政府內仍未加入 GSN/VPN 之資安機關加入內部整合網路，預計至少 10 個資安機關納入服務，以強化全縣資安防護網之完整性。
5. 骨幹網路安全防護，強化宜蘭縣政府及中興文創智慧聯網共用中心異地端資安設備共 4 台大型交換器及 6 台小型交換器，並建置分析網路速率系統。
6. 依資通安全管理法遵事項，完成 3 個 B 級機關導入端點偵測及應變機制，並提交端點偵測及應變機制偵測資料。
7. 依資通安全管理法遵事項，完成 10 個 C 級機關導入資安弱點通報機制。
8. 培訓本縣機關內部人員、本縣系統開發及維護有關之廠商系統人員、軟體工程師、資安相關科系學生，每年培訓人才至少 10 人次，完成培訓之人力可規劃後續參與本縣之紅藍攻防演練與滲透測試，強化本縣資安防護能力。

十二、相關聯絡資料

機關單位	姓名	電話	E-mail
新北市政府 資訊中心	羅國良	02-29603456#8554	AH1350@ntpc.gov.tw
新北市政府 資訊中心	辜仁杰	02-29603456#8547	AJ5157@ntpc.gov.tw
基隆市政府 綜合發展處	吳信東	02-24201122#1228	kl947@mail.klcg.gov.tw
基隆市政府 綜合發展處	王華田	02-24201122#1227	alainamedues@mail.klcg.gov.tw
基隆市政府 綜合發展處	周鈺惠	02-24201122＃1243	chou86898020@mail.klcg.gov.tw
宜蘭縣政府 計畫處	張炯明	03-9251000#3350	postit@mail.e-land.gov.tw
宜蘭縣政府 計畫處	陳長佑	03-9251000#3352	ccy@mail.e-land.gov.tw
宜蘭縣政府 計畫處	游文宏	03-9251000#3356	jamesbob@mail.e-and.gov.tw

附件3

政府基層機關資安主動防禦之分項計畫

桃園市政府(含新竹市、新竹縣、苗栗縣政府)

計畫全程：112年1月至113年12月

桃竹竹苗縣市政府
112 年-113 年度政府基層機關資安主動防禦計畫

一、 計畫緣起

因資訊電子化日漸擴增，政府與產業依賴電腦資訊系統也越深，資訊安全成為現代國家安全的重要環節，且配合行政院 112 至 113 年度「前瞻基礎建設計畫」，行政院資通安全處研提「政府基層機關資安主動防禦計畫」，推動資訊資源向上集中，持續強化資安防護能量，辦理滲透測試及紅藍軍攻防演練。

桃園市政府為精進地方政府資安防護能量，期藉由實質經費補助，導入政府機關資訊系統弱點通報系統(VANS)及端點偵測及應變機制(EDR)，以強化政府基層機關資安主動防禦能量，提升資通安全管理效能。新竹市政府為推動資訊資源向上集中，規劃辦理府外機關線路整併及建立完善之共用資料中心及異地備援環境，強化端點防護，落實資訊系統弱點通報機制，並培訓資安實戰人才，推動紅藍隊演練或資安檢測，期能有助於提升新竹縣政府網路資安環境並帶動資安產業發展。新竹縣政府為提升地方政府資安防護能量，期藉由實質經費補助，規劃朝資訊資源向上集中、精進資安防護能量及資安實戰人才培訓三大方向提升資通安全管理效能。此外，苗栗縣政府則規劃賡續推動政府資訊資源集中共享及推動資訊資源向上集中，持續強化資安防護能量，辦理資安實戰人才培訓及研提資通安全創新服務，期能有助於帶動資安產業發展。

桃園市政府結合新竹縣、新竹市及苗栗縣等鄰近區域縣市政府雖於 108 年至 110 年進行區域聯防機制之持續監控維運，但資安人力嚴重不足之問題仍持續存在；自 112 年起配合行政院資通安全處政策，研議規劃資訊資源向上集中之可行性，並搭配資安防護能量精進與實證場域資安實戰人才培訓，有效運用有限資源以避免過於分散，並持續強化整體資安防護力，與 N-ISAC 及 N-CERT 達到情資分享與建構更為穩固之國家資安監控網，特擬訂本計畫。

二、 計畫目標

因應資安問題日益嚴峻，駭客攻擊手法不斷創新及鄰近縣市資安防護人力的不足，從資安事件的早期預警、事件發生時快速協處改善、通報處理應變機制、以及平時的持續監控的角度，桃園市政府 107 年起已結合新竹縣、新竹市及苗栗縣等鄰近區域縣市政府部署資安區域聯防機制，將區域縣市政府之 SOC 及資安檢測、防毒、資料外洩防護、中央控管機制、入侵偵測系統授權更新等持續強化，並強化機關資安體質、結合鄰近縣市建立 SOC 區域聯防監控，俾利資安事件快速回應與處理。此外，規劃 ISAC 之服務項目、管理功能、報表功能，使用者管理、資安威脅情資通報機制、資安論壇、系統管理等機制，並實作於相關資訊平台內，除了發揮資安資訊分享與分析的功效之外，更能透過資安情資的資訊彙集、監控作業的執行、聯防共通介面的建立、資料備份計畫的執行，達到情報能見度、區域縣市政府分析能量分享、及快速行動的區域資安聯防建置目標，並與 N-ISAC 及其他 I-SAC 達到情資共享的目的。

108 年至 109 年間雖針對既有 107 年已部署完成之區域資安聯防監控網及技術資源共享機制進行後續之監控維運、賡續辦理市網/縣網網路整併、賡續強化基層機關資安防護體質等；雖提供完善的資訊安全設備，卻沒搭配具專業知識之資安人力，無法落實資訊安全之有效管理及稽核，故於 112 年至 113 年將評估規劃人力資源向上集中，透過建立桃園市政府專屬資安聯隊，除了給予教育訓練及專業證照課程培訓之外，藉由開辦交流工作坊，讓聯隊成員可互相分享各機關 ISMS 導入及稽核經驗，以提升整體團隊的管理能力，未來面臨資安事件時，可以更快之速度應變處理；並搭配網路、伺服器、ISMS 向上集中管理，精進資安防護能量及提供良好的實戰演練培訓以培育未來優秀之青年學子及專業人才，預計推動之計畫方向如下:

（一） 資訊資源向上集中

1. 網路整併(新竹市政府)
2. 建置共用資料中心(電腦機房)（新竹市政府）
3. 建置共用資料中心(虛擬化平台)（新竹市政府）
4. 整併地所資料中心至地政處(新竹市政府)

5. 因應各系統集中需配置之伺服器虛擬機環境建置(新竹縣政府)
6. 所屬網站整併、資料移轉(新竹縣政府)
7. 為民服務資訊匯流平台(新竹縣政府)
8. 單一簽入(員工入口網)(新竹縣政府)
9. 升級機房實體環境及基礎設備(苗栗縣政府)
10. 網路出口集中化(苗栗縣政府)
11. 系統集中化(苗栗縣政府)
12. 各項備援設備(含網路線路、設備備援)(苗栗縣政府)

(二) 精進資安防護能量

1. 導入政府機關資訊系統弱點通報系統(VANS)。
(桃園市政府、新竹市政府、新竹縣政府、苗栗縣政府)
2. 導入政府機關端點偵測及應變機制(EDR)
(桃園市政府、新竹市政府、新竹縣政府)
3. 網路流量加解密設備導入建置案(新竹縣政府)
4. 建置 DMZ 網路架構 HA 機制(新竹縣政府)
5. 向上集中佈建資安防護系統(新竹縣政府)
6. 區域聯防精進資安端點防護(苗栗縣政府)

(三) 推動滲透測試及紅藍軍攻防演練

1. 推動紅隊演練(新竹市政府)
2. 建置「共用資安攻防教育訓練平台系統」(新竹市政府)

三、 計畫內容與實施策略

(一) 桃園市政府

精進地方政府資安防護能量：

策略構想：

為持續強化及擴大桃園市政府資安防護機制，配合行政院資通安全處政策，於各資通安全責任等級C級之機關導入資訊系統弱點通報機制(VANS)及資通安全責任等級B級之機關導入端點偵測及應變機制(EDR)，並依資通安全管理法主管機關行政院資通安全處指定之方式提交端點偵測及應變機制(EDR)偵測資料，以利即

早發現資安弱點及資安威脅，即早處理，降低資安事件發生之機率，減少機關損害程度。

1. 導入政府機關資訊系統弱點通報系統(VANS)

(1) 策略重點：

為配合資通安全管理法規定機關應盤點資通系統，並建立相關風險評估機制，目前行政院國家資通安全會報技術服務中心推動政府機關資訊系統弱點通報系統，透過該系統可協助桃園市政府及其所屬機關落實資訊資產盤點與風險評估，以自動化方式進行弱點評估與修補作業；因桃園市政府現行的資產管理軟體可進行資產盤點機制，但無法產出 VANS 所制定之傳輸格式，透過將既有的資產軟體進行功能擴充後，即可匯出 VANS 所制定之格式。

(2) 現況說明：

桃園市政府原資產軟體可進行資產盤點機制，但無法產出 VANS 所制定之傳輸格式，爰於 110 年透過行政院資通安全處向行政院國家科學技術發展基金管理會申請補助經費，藉由該筆經費及桃園市政府自籌款，於桃園市政府暨所屬資通安全責任等級 6 個 B 級機關導入資訊系統弱點通報機制(VANS)，全案依規定已於 111 年 6 月底前完成導入。

桃園市政府暨所屬資通安全責任等級 C 級機關多達 60 個機關，為持續強化及擴大桃園市政府資安防護機制，囿於桃園市政府預算相當有限，亟需前瞻計畫經費補助，始能將資訊系統弱點通報機制(VANS) 導入各資通安全責任等級 C 級機關。

(3) 執行內容：

視補助經費額度於 112 年度針對桃園市政府暨所屬資通安全責任等級 C 級機關，導入 VANS。

2. 導入政府機關端點偵測及應變機制(EDR)

(1) 策略重點：

當未知攻擊在穿透資安設備的時候，並不會觸發任何的警報。在沒有任何警報的狀態下，不可能提前採取對應的行

動。過去傳統的處理方式只能被動等待，等到資安事件爆發，造成損失，才開始進行事後處理。因此在資安威脅初期，須能有一個採取主動收集分析資料，即時阻斷駭客活動，做到即時事件處理，大幅降低損失的軟體，故於個人電腦導入端點偵測及應變機制(EDR)即為可採用之解決方案。

(2) 現況說明：

桃園市政府因經費有限，於107-109年期間藉由前瞻計畫補助及桃園市政府自籌經費，目前6個資安責任等級B級機關除地方稅務局因預算不足僅導入100台個人電腦外，其餘5個已導入EDR機制，故若獲前瞻計畫經費補助，後續將以優先導入補足資安責任等級B級機關之個人電腦，倘有剩餘經費再陸續導入資安責任等級C級機關。

(3) 執行內容：

A. 112年度

無。

B. 113年度

(A) 部署桃園市政府暨所屬資通安全責任等級B級機關依資通安全管理法主管機關指定之方式提交端點偵測及應變機制(EDR)偵測資料之機制。

(B) 視補助經費額度賡續導入桃園市政府暨所屬資通安全責任等級C級機關。

(二) 新竹市政府

1. 資訊資源向上集中

(1) 網路整併

A. 策略重點：

(A) 線路整併：辦理本市所屬共計8個C級機關VPN線路整併，擴建光纖線路，並將各機關防火牆的日誌收納至本府的日誌系統，並納入本府SOC監控。此外本府共計21個所屬機關vpn 主幹線路目前僅有一條，將新增一條，以提供備援機制。

(B) 擴充網路基礎設施及備援資安設備：為因應資料向上

集中，資料中心減量之目標，本府各處暨所屬機關之系統及設備須移入本府機房，網路相關基礎設施須同步擴充，以強化機關資安設備之防護能力。此外，針對本府骨幹網路僅有一台之資安設備(應用程式防火牆及加解密設備等)，擬新購一台，除可達到備援機制亦可避免傳輸資料採用 SSL 加密流量時造成資安防範的另一個漏洞，提高本府基礎設施網路之安全性暨可用性。

(C) 建置遠端連線管控稽核平台：因應系統整併，原有之遠端連線控管軟體授權數及乘載能力恐無法負荷。故將擴充既有遠端連線容量及乘載力，此外並導入監控機制，以偵測攻擊與未授權之連線，透過平台詳細記錄遠端維護過程，針對不尋常或未授權之活動，針對該事件進行分析，此外並可做為日後稽核的重要依據。

(D) 建置系統日誌收納系統: 整併各機關之系統後，針對核心系統建置日誌收納系統，以雜湊或其他適當方式確保日誌之完整性，並於日誌處理失效時，提出告警機制。

(E) 建置惡意威脅智能鑑識系統:整併各機關之系統後，針對核心系統布建惡意威脅智能鑑識工具，以 AI 智能偵測、自動調查與自動聯防，掌握 APT 攻擊活動慣用伎倆、駭客後續攻擊階段中的入侵軌跡等，並可作為後續數位鑑識暨資安蒐證工具。

(F) 建置網路行為控管系統:針對前資安法要求之端點應遵循事項，如防毒、VANS、EDR 等進行控管，提前發現內網存在潛在風險之設備，提前進行矯正與處理，以鞏固本府端點之網路安全。

B. 執行內容：

(A) VPN 線路改由路由管理機制，並於 C 級機關出口增設防火牆。

(B) 因應資料向上集中，擴充機房網路基礎設備(switch、應用程式防火牆、加解密設備、日誌收容器擴增、分流負載平衡器)及備援資安設備(應用程式防火牆及加解密設備等)。

(C) 建置遠端連線管控稽核平台。

(2) 建置共用資料中心(電腦機房)

A. 策略重點：

現行本府資訊系統主機散落各局處單位存放，各局處存放系統設備環境並無具備「獨立存放之機房空間」、「伺服主機與個人電腦間防火牆或資安設備區隔防護」、「人員進出行門禁管控」、「環控、空調、消防及不斷電電力系統」等基本設施，為落實本府資安政策，規劃建置符合資安等級之共用資料中心電腦機房，將各局處資訊系統設備向上集中存放管理，以確保資訊系統機密性、完整性及可用性。

B. 執行內容：

(A) 建置下列具資安等級之電腦機房基礎環境設施，提供本府暨所屬機關單位伺服主機進駐。

a. 電力系統工程、空調、消防、環控系統建置

b. 光纖網路及機房網路佈線

c. 機房擴增工程

(B) 本府暨所屬機關目前共計 14 個資料中心（行政處、交通處、地政處*2、都發處、社會處、警察局、稅務局、消防局、衛生局、文化局、地政事務所、殯葬管理所、家庭教育中心)，規劃 112 年度擴建資訊科電腦機房資料中心基礎設施，113 年度將各局處資料中心設備向上集中收納到資訊科電腦機房資料中心管理，預計可縮減 9 個資料中心（餘 5 個資料中心，除資訊科資料中心外，其餘 4 個警政、稅務、消防、地政等中央系統資料中心暫不列入收納範圍)。

(3) 建置共用資料中心(虛擬化平台)

A. 策略重點：

現行各局處應用系統及設備分散在各地，規劃建置共用資料中心虛擬化平台，提供各局處應用系統安裝使用，強化設備資訊安全控管，達到集中化管理目標，降低各局處自行購置及管理資訊系統之成本及資安風險。此外，為因應資料向上集中，擴增資料中心基礎環境(含異地備援)設施。

B. 執行內容：

(A) 本府暨所屬機關目前共計 130 個系統平台，規劃 112-113 年度擴建虛擬化平台(含異地備援)設備，建置共用資料中心收納各局處伺服主機，預計 112 年度起每年向上集中收納 3~5 個單位伺服主機服務到共用資料中心，搭配整併線路集中網路出口及落實網段區隔，大幅縮減資安防護缺口。

(B) 虛擬化平台及異地備援環境基礎設施擴增(包括備份主機及軟體、高階儲存設備、虛擬化作業環境等。)

(4) 整併地所資料中心至地政處

A. 策略重點：

(A) 地政事務所核心資訊系統向上集中到地政處管理。

(B) 因應資料向上集中，改善資料中心與異地備援中心基礎環境，並配合異地備援中心作業需求，建置備援中心資安防護基礎設施。

B. 執行內容：

(A) 提升資料中心與異地備援中心基礎環境運作效能及容錯能力：因應資料向上集中，改善資料中心與異地備援中心基礎環境，包括資料庫主機、高階儲存設備、虛擬化作業環境等。

(B) 建置異地備援中心資安防護基礎設施：配合異地備援中心作業需求，建置備援中心資安防護基礎設施，包括防火牆、入侵偵測系統等設備。

(C) 網路及伺服主機監控與區域聯防告警平台規劃建置：建置網路設備與線路監控與告警平台並完成網路氣象

圖繪製及設定調校，集中儲存 SNMP、Syslog、網路流量管理等資料功能及製作各種管理報表功能。

(D) 連線管控稽核平台規劃建置：建置遠端連線管控稽核平台，透過平台詳細記錄遠端維護過程，做為日後稽查歸檔或線上可以在第一時間過濾指令的重要依據，以滿足本處機房管理安全以及 ISMS 和個資法所要求之法律規範。

(E) 資料庫稽核：建置具備事前預防、事中證據保存、事後稽核的安全控管，當應用程式或終端設備欲對資料庫進行操作，可提供如開放(禁止)特定 IP 之存取、SQL 指令之側錄、報表之產出等，確保並維護資料庫安全，滿足地政機房管理安全以及 ISMS 和個資法所要求之法律規範。

2. 精進資安防護能量

(1) 推動政府機關資訊系統弱點通報機制(VANS)

A. 策略重點：

為落實資訊系統弱點通報機制，於本府暨所屬機關端點電腦安裝資產管理軟體，建置管控中心平台進行資產統計分析，以及將資料回傳至行政院資訊系統弱點通報監控中心，即時針對監控中心通報弱點進行用戶端電腦系統弱點修補，強化端點電腦資安防護作業。

B. 執行內容：

本府共計 2 個 B 級機關，8 個 C 級機關，規劃將個人電腦設備及伺服器導入資訊系統弱點通報平台，定期將軟體資訊傳送到政府機關資訊系統弱點通報 VANS 系統平台進行分析，並針對風險較高的弱點建立快速派送修補機制，目前約須 2,450 台 vans 軟體授權。

(2) 推動端點偵測及應變機制(EDR)

A. 策略重點：

為落實資通安全管理法之應辦事項，佈署端點威脅防禦系統，採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，以利加速採證及資安鑑識作業。

B. 執行內容：

本府共計 2 個 B 級機關，共計約 1,700 台個人電腦及伺服器設備，規劃依資安法規範導入 EDR 偵測及應變機制，針對端點設備惡意程式偵測阻擋並建立資安事件鑑識分析機制。

3. 推動滲透測試及紅藍軍攻防演練

（1）策略重點：

A. 推動紅隊演練(如網站與主機、IOT 測試、邊界探測、內網橫向入侵等)一次或滲透測試至少 30 個網站，由本府提供實證場域，讓第三方業者模擬駭客實際攻擊本府對外服務系統或連網設備。在紅隊攻擊同時，會進行黑箱/灰箱的攻防測試，預計整體花費時間超過 3 個月。過程中將進行無邊界的調查及確認範圍等作業，待修補完成後，實施一次複測，以檢驗相關漏洞修補狀況，並出具複測驗證報告。

B. 建置「共用資安攻防教育訓練平台系統」，辦理多場的紅藍隊資安攻防教育訓練課程，讓本府各資安窗口能參與實際的紅藍隊資安攻防演練。

（2）執行內容

A. 紅藍隊攻防練一次或滲透測試至少 30 個網站。

B. 建置「共用資安攻防教育訓練平台系統」並辦理教育訓練培訓人才至少 30 人次。

（三） 新竹縣政府

1. 資訊資源向上集中

（1）因應各系統集中需配置之伺服器虛擬機環境建置

A. 策略重點：

提供本府及所屬機關集中之虛擬環境及備援機制，強化系統之可用性，硬體主機可集中管理減低管理人員之負擔。

B. 執行內容：

於本府資訊機房建構虛擬主機及備援機制，實體主機之資訊系統移轉至虛擬環境， 提供穩定之運轉環境，降低管理及維護成本。

(2) 所屬網站整併、資料移轉

A. 策略重點：

針對本府及所屬機關全球資訊網進行整併，以達到向上集中管理及訊息互通。

B. 執行內容：

整併本府及所屬機關中英文官網。

(3) 為民服務資訊匯流平台

A. 策略重點：

統整本府縣民信箱、話務中心 1999 和陳情 APP...等多種管道民眾意見，藉此平台派送各局處及公所等單位處理後，期限內回覆民眾，使民意有效傳達。

B. 執行內容：

(A) 匯整本府各種管道民眾陳情意見。

(B) 陳情類別項目盤點確認，流程整併調整。

(C) 前後台網頁跨瀏覽器支援並提升資安防護。

(D) 整併所屬民眾信箱。

(4) 單一簽入(員工入口網)

A. 策略重點：

現行員工入口網採單一簽入平台認證後即可存取多個應用程式的功能，具有跨平台、即時性整合性帳號及權限管理機制，本計畫預計強化系統資通安全之強度，並建置共用行政輔助系統例如：文具請領、會議室借用及公務車借用...等預計擴充功能，以提供本縣公務機關使用。

B. 執行內容：

(A) 提供各應用系統與員工入口網單一簽入介接之功能 (Web service or API 等)。

(B) 擴充共用行政輔助系統。

(C) 強化系統各項資安防護控制措施。

(D) 至少整併納入本縣 6 個公務機關。

2. 精進資安防護能量

(1) 網路流量加解密設備導入建置案

A. 策略重點：

針對整併架構中的所有網路連線流量加解密，以確認是否有惡意的連線隱藏在加密連線中，提高網路可視性、提升資安設備防禦效果。

B. 執行內容：

導入設備後，本府及所屬機關單位個人電腦均安裝網路流量加解密設備自簽憑證。

(2) 建置 DMZ 網路架構 HA 機制

A. 策略重點：

重新規劃設計 DMZ 伺服器群，且依據風險等級、服務屬性劃分區域及改善原有設計單點失效問題。

B. 執行內容：

預計佈署設備臺數：核心交換器*1、伺服器交換器*20。

(3) 導入資訊系統弱點通報機制(VANS)

A. 策略重點：

為強化資通訊資產弱點防護能力，推動縣府導入政府機關資安弱點通報機制。

B. 執行內容：

(A) 整合縣府、警察局及稅務局現在資產管理系統上傳 CPE 格式資訊資產清單。

(B) 於 VANS 系統進行資訊資產管理與風險管理。

(C) 透過電子郵件接收 VANS 系統發送之弱點通知。

(D) 至 VANS 系統進行弱點確認與修補規劃，並更新資訊資產。

(4) 導入端點偵測及應變機制(EDR)

A. 策略重點：

為強化端點偵測及應變防護能力，推動本縣 B 級機關導入端點偵測及應變機制。

B. 執行內容：

本府使用目錄伺服器群組原則物件派發安裝代理程式，府外機關撰寫腳本安裝代理程式。

(5) 向上集中佈建資安防護系統

A. 策略重點：

針對線路整併後統一部屬集中式威脅管理防火牆，控管88個外部單位，提供威脅防禦、網址過濾、惡意軟體分析。

B. 執行內容：

本府及所屬機關因網路整併後，原有設備效能及連線日誌儲存均受影響，故需依大量連線數重新評估佈建防火牆。

(四) 苗栗縣政府

1. 資訊資源向上集中

規劃目標	1. 衛生局、18衛生所、苗栗縣政府毒品防制及心理衛生中心、苗栗縣政府長期照護管理中心對外網路收容至本府統一出口。 2. 將衛生局、18衛生所、苗栗縣政府毒品防制及心理衛生中心、苗栗縣政府長期照護管理中心所有資訊系統集中至本府機房統一管理。 3. 導入共用之電子郵件、統一員工入口網及全球資訊網等系統。
工作大綱	1. 整併網路線路。 2. 建置共用資料中心(機房)。 3. 建置及推廣共用性系統。
執行順序	1. 系統集中化管理：超融合實體設備、軟體授權、雲端化管理系統、實體轉虛擬、各單位環境調整、老舊系統重新開發、系統負載平衡...。 2. 升級機房實體環境：結構化佈線系統、精密式空調系統、環境監控系統安裝、不斷電系統、UPS不斷電電力系統、機房備援電力系統建置、及時設備盤查系統。 3. 網路集中化管理：線路網路整併、VPN建置、VPN CORE線路、網路調整、線路負載平衡、出口線路、備援線路、...等。 4. 提升網路設備基礎設備：汰換老舊設備及增加相關設備如：防火牆、交換器、路由器、網路分流設備，以利收

	容後，避免有效能不足問題。 5. 網頁應用防火牆：建置網頁應用防火牆，避免收容後效能不足問題。 6. 建立異地備份機制。

2. 精進資安防護能量

規劃目標	1. 為精進基層機關端點防護能量，導入端點威脅防禦系統(EDR)，俾利了解基層機關發生資通安全事件的相關歷程。 2. 導入政府機關資訊系統弱點通報機制(VANS)，並推廣至本府 C 級機關。
工作大綱	1. 導入端點威脅防禦系統(EDR)。 2. 推廣政府機關資訊系統弱點通報機制(VANS)。
執行順序	1. 導入端點威脅防禦系統(EDR)。 2. 推廣政府機關資訊系統弱點通報機制(VANS)。

四、 實施範圍

本計畫實施對象為桃園市政府、新竹市政府、新竹縣政府及苗栗縣政府暨所屬機關，並依行政院資通安全處規定以資通安全責任等級 B 級及 C 級機關為優先導入資訊系統弱點通報機制及端點偵測及應變機制之實施對象。

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

（一） 桃園市政府

年度	項次	關鍵績效指標	目標值
112	1	資通安全責任等級 C 級機關導入介接 VANS 導入率(導入 C 級機關個數/C 級機關總數，C 級機關總數 60 個)	100%
113	1	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率(導入 B 級機關個數/B 級機關總數，B 級機關總數 6 個)	100%

（二） 新竹市政府

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	2
	2	資通安全責任等級 BC 級機關導入介接 VANS 導入率(導入 BC 級機關個數/BC 級機關總數，BC 級機關總數 10 個)	100%
	3	資通安全責任等級 B 級機關導入 EDR 導入率(導入 B 級機關個數/B 級機關總數，B 級機關總數 2 個)	100%
	4	攻防演練培訓人才或滲透測試網站數	30
113	1	完成資料中心減量個數	7
	2	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率(B 級機關提交個數/B 級機關總數，B 級機關總數 2 個)	100%
	3	攻防演練培訓人才或滲透測試網站數	30

（三） 新竹縣政府

年度	項次	關鍵績效指標	目標值
112	1	資通安全責任等級 C 級機關導入介接 VANS 導入率(導入 C 級機關個數/C 級機關總數，C 級機關總數 21 個)	100%
	2	資通安全責任等級 B 級機關導入 EDR 導入率(導入 B 級機關個數/B 級機關總數，B 級機關總數 3 個)	100%
113	1	完成資料中心減量個數	4
	2	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率(導入 B 級機關個數/B 級機關總數，B 級機關總數 3 個)	100%

（四） 苗栗縣政府

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	5
	2	資通安全責任等級 C 級機關導入介接 VANS 導入率(導入 C 級機關個數/C 級機關總數，C 級機關總數 10 個)	100%
	3	資通安全責任等級 B 級機關導入 EDR 導入率(導入 B 級機關個數/B 級機關總數)	100%
113	1	完成資料中心減量個數	16

	2	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率(導入B級機關個數/B級機關總數，B級機關總數3個)	100%

七、 持續營運評估

（一） 桃園市政府

112至113年由本案計畫經費支應，於計畫期程結束後，維運及服務模式評估持續以委外服務案方式，後續行政院若無繼續補助發展經費時，將賡續爭取逐年提列相關維護營運費用以為支應，期能持續提升整體資安防護力。

（二） 新竹市政府

本計畫期程結束後，後續維運及服務模式評估持續以委外服務案方式，經費則由地方政府編列預算動支。此外，本案透過相關人才之培育及產學合作模式，希望於計畫結束後藉由專業分工合作方式進行策略聯盟，發揮培育綜效。

（三） 新竹縣政府

新竹政府結合桃園市、新竹市及苗栗縣等鄰近區域縣市政府於前瞻計畫第一、二期完成區域聯防機制部署並持續營運，在該基礎上將於112年至113年以辦理資訊資源向上集中、精進資安防護能量，研提其他創新服務，及資安人才培訓等策略面向，推動建置共用資料中心，資訊向上集中，建置必要之資安防護，備援機制，結合高等學院提供訓練等，未來透過相關人才之培育及產學合作模式，希望於計畫結束後持續藉由專業分工合作方式進行策略聯盟，發揮互動互助產官學良性綜效，後續行政院若無繼續補助發展經費時，將賡續爭取逐年提列相關維護營運費用以為支應，期能持續提升本府整體資安防護力。

（四） 苗栗縣政府

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	整併網路線路	線路費	由本府及各使用機關每年編

	上集中			列預算支應：每年約 120 萬元。
2		建置共用系統	維護費	由本府及各使用機關每年編列預算支應：每年約 300 萬元。
3		區域聯防精進	系統授權及維護	由本府及各使用機關每年編列預算支應：每年約 1000 萬元。

八、 經費明細概算

（一） 桃園市政府

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	導入政府機關資訊系統弱點通報系統(VANS)	視補助經費額度於 112 年度針對桃園市政府暨所屬資通安全責任等級 C 級機關，導入 VANS	10,908,333	1,687,500	符合資通安全責任等級 C 級之機關均導入資訊系統弱點通報機制(VANS)。	1
112 年度小計				10,908,333	1,687,500		
112 年度合計				12,595,833			

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	導入政府機關端點偵測及應變機制(EDR)	部署桃園市政府暨所屬資通安全責任等級B級機關依資通安全管理法主管機關指定之方式提交端點偵測及應變機制(EDR)偵測資料之機制。	1,200,000	1,500,000	符合資通安全責任等級B級之地方政府均導入端點偵測及應變機制(EDR)。	1
			視補助經費額度賡續導入桃園市政府暨所屬資通安全責任等級C級機關。	2,586,667	412,500		2
113年度小計				3,786,667	1,912,500		
113年度合計					5,699,167		

（二） 新竹市政府

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	網路整併	辦理本市所屬C級8個機關VPN線路整併、電路改接服務、端點IP及路由改接、資安暨路由設備購置及維護、建置遠端連線管控	9,071,429	6,550,000	1. 本市所屬C級8個機關VPN線路整併。 2. 本市9個機關資料中心向上集中至機房。	2

			稽核平台、建置系統日誌收納系統、建置惡意威脅智能鑑識系統、建置網路行為控管系統。				
	2	建置共用資料中心（電腦機房）	1. 建置共構機房之電力工程、空調系統、消防系統、環控系統及光纖網路工程等。 2. 各局處資訊機房及系統設備向上集中到資訊科共構機房存放。	8,000,000	18,000,000	本府暨所屬機關共計14個資料中心（行政處、交通處、地政處*2、都發處、社會處、警察局、稅務局、消防局、衛生局、文化局、地政事務所、殯葬管理所、家庭教育中心），規劃112年度擴建資訊科電腦機房資料中心基礎設施，113年度將各局處資料中心設備向上集中收納到資訊科電腦機房資料中心管理，預計可縮減9個資料中心（餘5個資料中心，除資訊科資料中心外，其餘4個警政、稅務、消防、地政等中央系統資料中心暫不列入收納範圍）。	6
	3	建置共用資料中心（虛擬	建置共用資料中心提供各局處應用系統移入共		6,550,000	本府暨所屬機關目前共計130個系統平台，規劃112年度擴建虛	4

		化平台）	用 VM 平台執行。			擬化平台設備，建置共用資料中心收納各局處伺服主機，預計 112 年度起每年向上集中收納 3~5 個單位伺服主機服務到共用資料中心，搭配整併線路集中網路出口及落實網段區隔，大幅縮減資安防護缺口。	
	4	整併地所資料中心至地政處	1. 強化資料中心並整併所需之資安防護設備。 2. 建立異地備援機制。		1,600,000	地政資訊資源向上集中化。	5
	5	推動政府機關資訊系統弱點通報機制(VANS)	用戶端個人電腦及伺服器安裝資產管理軟體，並將相關資訊回傳中央 VANS 系統	1,000,000	0	預計 112 年度完成 BC 級機關共計 2,450 台 pc 及 server 完成資訊系統弱點通報佈署。	3
	6	推動端點偵測及應變機制(EDR)	用戶端個人電腦及伺服器安裝端點偵測及應變軟體。	3,000,000	0	預計 112 年度完成 B 級機關共計 1,450 台 pc 及 server 完成資訊系統弱點通報佈署。	1
	7	推動滲透測試及紅藍軍攻防演練	規劃紅藍隊攻防演練及資安檢測，並培訓相關人才或滲透測試執行至少 30 個網	6,000,000	0	1. 推動紅藍隊攻防演練每年一次或資安檢測至少 6 案。 2. 培訓紅藍隊資安攻防人才至少 30 人次或	7

			站。			滲透測試執行至少 30 個網站。	
112 年度小計				27,071,429	32,700,000		
112 年度合計				59,771,429			

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	網路整併	1. 因應資訊向上集中，擴充基礎設施。 2. 建置遠端連線管控稽核平台，加強遠端連線安全性。	4,350,000	8,000,000	1. 因應資訊向上集中，擴充基礎設施。 2. 本府 36 個機關單位之委外廠商均可透過共用性遠端連線系統進行連線。	2
	2	建置共用資料中心(電腦機房)	1. 建置共構機房之電力工程、空調系統、消防系統、環控系統及光纖網路工程等。 2. 各局處資訊機房及系統設備向上集中到資訊科共構機房存放。	0	10,000,000	本府暨所屬機關共計 14 個資料中心（行政處、交通處、地政處*2、都發處、社會處、警察局、稅務局、消防局、衛生局、文化局、地政事務所、殯葬管理所、家庭教育中心)，規劃 112 年度擴建資訊科電腦機房資料中心基礎設施，113 年度將各局處資料中心設備向上集中收納到資訊科電腦機房資料中心管理，預計可縮減 9 個資料中心（餘 5 個資料中心，除資訊科資料中心外，其餘 4 個警政、稅	6

						務、消防、地政等中央系統資料中心暫不列入收納範圍)。	
	3	擴充共用資料中心(虛擬化平台)	建置共用資料中心提供各局處應用系統移入共用 VM 平台執行	0	5,600,000	每年向上集中收納 3~5 個單位伺服主機服務到共用資料中心，搭配整併線路集中網路出口及落實網段區隔，大幅縮減資安防護缺口	4
	4	整併地所資料中心至地政處	1. 強化資料中心並整併所需之資安防護設備。 2. 建立異地備援機制。	0	2,500,000	地政資訊資源向上集中化	5
	5	推動政府機關資訊系統弱點通報機制(VANS)	用戶端個人電腦及伺服器安裝資產管理軟體，並將相關資訊回傳中央 VANS 系統。	1,000,000	0	預計 113 年度持續維運 BC 級機關共計 2,450 台 pc 及 server 弱點通報機制。	3
	6	推動端點偵測及應變機制(EDR)	用戶端個人電腦及伺服器安裝端點偵測及應變軟體。	3,000,000	0	預計 113 年度持續維運 B 級機關共計 1,450 台 pc 及 server 完成資訊系統弱點通報佈署。	1
	7	推動滲透測試及紅藍軍攻防演練	規劃紅藍隊攻防演練及資安檢測，並培訓相關人才或滲透測試執行至少 30 個網站。	6,000,000	0	1. 推動紅藍隊攻防演練每年一次或資安檢測至少 6 案。 2. 培訓紅藍隊資安攻防人才至少 30 人次或滲透測試執行至少 30 個網站。。	7
113 年度小計				14,350,000	26,100,000		
113 年度合計					40,450,000		

（三） 新竹縣政府

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	1-1	因應各系統集中需配置之伺服器虛擬機環境建置	提供本府及所屬集中之虛擬環境及備援機制，強化系統之可用性，硬體主機可集中管理減低管理人員之負擔。	0	11,600,000	1. 因應資訊向上集中，擴充基礎設施。 2. 本府及所屬至少6個機關單位可用集中之虛擬環境及備援機制。	5
	1-2	所屬網站整併、資料移轉	針對本府及所屬機關全球資訊網進行整併，以達到向上集中管理及訊息互通，建置共通平台，向上集中控管維運，建立備援機制。	0	5,000,000	所屬至少2個機關全球資訊網進行整併，建置共通平台，向上集中控管維運，建立備援機制。	7
	1-4	單一簽入(員工入口網)	建立員工入口網採單一簽入平台認證後即可存取多個應用程式的功能，具有跨平台、即時性整合性帳號及權限管理機制，並建置共用行政輔助系統。	0	6,100,000	完成建立本府及所屬員工入口網採單一簽入平台認證後即可存取多個應用程式的功能，並建置本府共用行政輔助系統。	6

	2-1	網路流量加解密設備導入建置案	針對整併架構中的所有網路連線流量加解密，以確認是否有惡意的連線隱藏在加密連線中，提高網路可視性、提升資安設備防禦效果。	2,800,000		針對88個外部單位向上集中整併架構中的所有網路連線流量加解密，以確認是否有惡意的連線隱藏在加密連線。	8
	2-2	建置 DMZ 網路架構 HA 機制	重新規劃設計 DMZ 伺服器群，且依據風險等級、服務屬性劃分區域及改善原有設計單點失效問題。	0	1,000,000	所屬88個外部單位向上集中，集中後依據風險等級、服務屬性劃分區域及改善原有設計單點失效問題。	11
	2-3	導入資訊系統弱點通報機制(VANS)	為強化資通訊資產弱點防護能力，推動縣府導入政府機關資安弱點通報機制。	5,200,000	0	預計112年度完成C級機關共計2,500台pc及server之資訊系統弱點通報機制佈署。	1
	2-4	導入端點偵測及應變機制(EDR)	為強化端點偵測及應變防護能力，推動本縣B級機關導入端點偵測及應變機制(EDR)。	3,200,000	0	預計112年度完成B級機關共計1,600台pc及server之端點偵測及應變機制佈署。	2
	2-5	向上集中佈建資安防護系統	針對線路整併後統一部屬集中式威脅管理防火牆，控管88個外部單	3,000,000	3,000,000	所屬網路向上集中後，統一部屬集中式威脅管理防火牆，控管88個外部單位，部署防火牆100%，統一維運。	4

			位，提供威脅防禦、網址過濾、惡意軟體分析。				
112 年度小計				14,200,000	26,700,000		
112 年度合計					40,900,000		

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	1-1	因應各系統集中需配置之伺服器虛擬機環境建置	提供本府及所屬集中之虛擬環境及備援機制，強化系統之可用性，硬體主機可集中管理減低管理人員之負擔。	0	11,600,000	1.因應資訊向上集中，擴充基礎設施。 2.本府及所屬機關單位可用集中之虛擬環境及備援機制。	9
	1-2	所屬網站整併、資料移轉	針對本府及所屬機關全球資訊網進行整併，以達到向上集中管理及訊息互通，向上集中控管維運，建立備援機制。	0	5,000,000	所屬至少 6 個機關全球資訊網進行整併，向上集中控管維運，建立備援機制。	12
	1-3	為民服務資訊匯流平台	統整本府縣民信箱、話務中心 1999 和陳情 APP...等多種管道民眾意見，藉此	0	6,000,000	所屬至少 6 個機關民眾信箱系統進行整併，向上集中控管維運，並建立備援機制。	14

			平台派送各局處及公所等單位處理後，於期限內回覆民眾，使民意有效傳達。				
	1-4	單一簽入(員工入口網)	建置所屬共用行政輔助系統	0	1,000,000	所屬至少 6 個機關向上集中加入共用行政輔助系統。	13
	2-1	網路流量加解密設備導入建置案	針對整併架構中的所有網路連線流量加解密，以確認是否有惡意的連線隱藏在加密連線中，提高網路可視性、提升資安設備防禦效果。	1,500,000	8,000,000	針對 88 個外部單位向上集中整併架構中的所有網路連線流量加解密，以確認是否有惡意的連線隱藏在加密連線。	10
	2-2	建置 DMZ 網路架構 HA 機制	重新規劃設計 DMZ 伺服器群，且依據風險等級、服務屬性劃分區域及改善原有設計單點失效問題。	0	1,000,000	所屬 88 個外部單位向上集中，集中後依據風險等級、服務屬性劃分區域及改善原有設計單點失效問題。	16
	2-4	導入端點偵測及應變機制(EDR)	為強化端點偵測及應變防護能力，推動本縣 B 級機關導入端點偵測及應變機制(EDR)。	3,200,000	0	預計 113 年度持續營運 B 級機關共計 1,600 台 pc 及 server 之端點偵測及應變機制，且提交率達 100%	3
	2-5	向上集中佈建資安防護系統	針對線路整併後統一部屬集中式威	3,000,000	0	所屬網路向上集中後，統一部屬集中式威脅管理防火	15

			脅管理防火牆，控管88個外部單位，提供威脅防禦、網址過濾、惡意軟體分析。			牆，控管88個外部單位，部署防火牆100%，統一維運。	
113年度小計				7,700,000	32,600,000		
113年度合計					40,300,000		

（四） 苗栗縣政府

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	升級機房實體環境	結構化佈線系統、精密式空調系統、環境監控系統安裝、不斷電系統、UPS不斷電電力系統、機房備援電力系統建置、及時設備盤查系統。	2,000,000	4,000,000	完成所屬21個機關進行資訊資源向上集中規劃及施作並辦理重複之行政必要系統。	2
	2	提升網路設備基礎設備	防火牆、交換器、路由器、網路分流設備。	3,433,000	3,928,194	完成所屬21個機關進行資訊資源向上集中規劃及施作並辦理重複之行政必要系統。	4
	3	系統集中化管理	超融合實體設備、軟體授權、雲端化管理系統、實體轉虛擬、各單位環境調整、老舊系統重新	10,998,256	7,400,000	完成所屬21個機關進行資訊資源向上集中規劃及施作並辦理重複之行政必要系統。	1

			開發、系統負載平衡... 。				
	4	網路集中化管理	線路網路整併、VPN 建置、VPN CORE 線路、網路調整、線路負載平衡、出口線路、備援線路、...等。	2,200,000	0	完成所屬 21 個機關進行資訊資源向上集中規劃及施作並辦理重複之行政必要系統。	3
	5	各項備援設備基礎設備	雲端備份、異地備援主機硬體設備、異地備援各系統軟體、異地備援網路設備、異地備援資安防護設備、異地備援線路。	3,000,000	0		8
	6	網頁應用防火牆	建置網頁應用防火牆。	4,000,000	0	完成所屬 21 個機關進行資訊資源向上集中規劃及施作並辦理重複之行政必要系統。	7
	7	端點威脅防禦系統	導入端點威脅防禦系統。	5,000,000	0	符合資通安全責任等級 B 級之地方政府均導入端點偵測及應變機制(EDR)。	6
	8	政府機關資訊系統弱點通報及配套機制建置	機關 VANS 輔導作業。	5,000,000	0	資通安全責任等級C級機關導入資訊系統弱點通報機制(VANS)。	5
112 年度小計				35,631,256	15,328,194		
112 年度合計					50,959,450		

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	升級機房實體環境	結構化佈線系統、環境監控系統安裝、不斷電系統、UPS 不斷電電力系統、機房備援電力系統建置、及時設備盤查系統。	3,692,422	5,000,000	完成所屬 21 個機關進行資訊資源向上集中規劃及施作並辦理重複之行政必要系統。	1
	2	提升網路設備基礎設備	防火牆、交換器、路由器、網路分流設備。	4,000,000	13,640,148	完成所屬 21 個機關進行資訊資源向上集中規劃及施作並辦理重複之行政必要系統。	2
	3	系統集中化管理	超融合實體設備、軟體授權、雲端化管理系統、實體轉虛擬、各單位環境調整、老舊系統重新開發、系統負載平衡..。.	11,000,000	10,186,400	完成所屬 21 個機關進行資訊資源向上集中規劃及施作並辦理重複之行政必要系統。	3
	4	網路集中化管理	線路網路整併、VPN 建置、VPN CORE 線路、網路調整、線路負載	4,660,000	1,000,000		4

			平衡、出口線路、備援線路、...等。				
	5	各項備援設備基礎設備	雲端備份、異地備援主機硬體設備、異地備援各系統軟體、異地備援網路設備、異地備援資安防護設備、異地備援線路。	3,000,000	3,717,600	完成所屬 21 個機關進行資訊資源向上集中規劃及施作並辦理重複之行政必要系統。	5
	6	網頁應用防火牆	建置網頁應用防火牆。	4,000,000	0		6
	7	端點威脅防禦系統	導入端點威脅防禦系統。	5,500,000	0	符合資通安全責任等級 B 級之地方政府均導入端點偵測及應變機制(EDR)。	7
113 年度小計				35,852,422	33,544,148		
113 年度合計					69,396,570		

九、 經費補助表

（一） 桃園市政府

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	12,595,833	0	5,038,333	7,557,500
113 年	5,699,167	0	2,279,667	3,419,500

（二） 新竹市政府

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	59,771,429	0	17,931,029	41,840,400
113 年	40,450,000	0	12,135,000	28,315,000

（三） 新竹縣政府

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	40,900,000	0	12,270,000	28,630,000
113 年	40,300,000	0	12,090,000	28,210,000

（四） 苗栗縣政府

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 **（補至千位數）**	行政院補助款
112 年	50,959,450	0	5,096,000	45,863,450
113 年	69,396,570	0	6,940,000	62,456,570

十、 預定進度

（一） 桃園市政府

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
112/12	100%	12,595,833	符合資通安全責任等級 C 級之機關中導入資訊系統弱點通報機制(VANS)之機關比率達 100%

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
113/12	100%	5,699,167	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率(導入 B 級機關個數/B 級機

			關總數，B 級機關總數 6 個）

（二） 新竹市政府

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
112/11	100%	59,771,429	1. 完成資料中心減量 2 個。 2. 資通安全責任等級 BC 級機關導入介接 VANS 導入率達 100%(導入 BC 級機關個數/BC 級機關總數，BC 級機關總數 10 個） 3. 資通安全責任等級 B 級機關導入 EDR 導入率達 100%(導入 B 級機關個數/B 級機關總數，B 級機關總數 2 個)。 4. 培訓人才至少 30 人次或辦理滲透測試至少 30 個網站。

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
113/11	100%	40,450,000	1. 完成資料中心減量 7 個。 2. 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率達 100%(B 級機關提交個數/B 級機關總數，B 級機關總數 2 個)。 3. 培訓人才至少 30 人次或辦理滲透測試至少 30 個網站。

（三） 新竹縣政府

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
112/6	25%	0	完成採購程序。
112/9	75%	30,675,000	1. 完成 15 個 C 級機關導入介接 VANS。 2. 完成 2 個 B 級機關導入 EDR。
112/12	100%	40,900,000	1. 完成 21 個 C 級機關導入介接 VANS。 2. 完成 3 個 B 級機關導入 EDR。

時程	累計預定	累計預定支	關鍵查核點

	進度(%)	用費用(元)	
113/6	25%	0	完成採購程序。
113/9	75%	30,225,000	完成 2 個 B 級機關提交 EDR 至主管機關指定位置。
113/12	100%	40,300,000	1. 完成 4 個資料中心減量個數。 2. 完成 3 個 B 級機關提交 EDR 至主管機關指定位置。

（四） 苗栗縣政府

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
112/8	40%	20,383,780	1. 整併第 3 個機房。 2. MDR 導入 3 個機關。

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
113/8	65%	78,231,413	1. 整併第 10 個機房（累計 15 個機房）。 2. 提交 3 個機關 MDR 資料至主管機關指定位置。

十一、 預期效益

（一） 桃園市政府

精進地方政府資安防護能量

1. 以往漏洞修補頻率遠低於駭客掃描探測的頻率，讓駭客有機可乘，為防止系統與軟體漏洞被駭客所利用，唯有透過有效率的漏洞修補工具，縮短被駭客利用之空窗期，降低資安風險。導入政府機關資訊系統弱點通報系統(VANS)，透過該系統可協助桃園市政府及其所屬機關落實資訊資產盤點與風險評估，以自動化方式進行弱點評估與修補作業，節省可能耗費之大量人力及時間，降低資安威脅及機關遭受損害。
2. 導入政府機關端點偵測及應變機制(EDR)可使機關在資安威脅初期，就能採取主動收集分析資料，即時阻斷駭客活動，做

到即時事件處理，大幅降低機關損失。

（二） 新竹市政府

1. 推動資訊資源向上集中及資料中心建置，以有效運用有限資源以避免過於分散。
2. 賡續辦理市網/縣網網路整併、建置遠端連線管控稽核平台、日誌收納系統、惡意威脅智能鑑識系統及網路行為控管系統，賡續強化基層機關資安防護體質。
3. 辦理攻防演練或滲透測試，提升府內資安窗口對資安事件之預警與應處能力並提升本府網路及資安防護之深度。
4. 導入政府機關資安弱點通報機制及端點偵測及應變機制，強化端點設備資安防護能力，針對即時惡意行為偵測、分析阻擋，並可完整分析攻擊資訊。

（三） 新竹縣政府

1. 資訊資源向上集中，精進資安防護能量。
2. 提升地方政府對資安事件之預警與應處能力。
3. 導入政府機關資安弱點通報機制，強化資通訊資產弱點防護能力。
4. 強化資安防護設備，減少重大資安事件發生率。

（四） 苗栗縣政府

1. 所屬 21 個機關進行資訊資源向上集中規劃及施作並辦理重複之行政必要系統（如電子郵件、統一員工入口網、公文…等系統）改以本府共用性系統取代及所屬機關之各別資訊系統集中移置本府共構機房，由本府進行統一管理資訊流進出口，加強防護，減少 21 個機關有相同資安設備重複設置浪費，使資源有效利用，更可大幅降低所屬 21 個機關防護能量不足之問題，讓 21 個機關可達到資通安全責任等級 B 級之防護能力
2. 導入端點威脅防禦系統，俾利了解基層機關發生資通安全事件的相關歷程，從端點防護出發，預期達到即時惡意行為偵測與分析、即時資安事件處理、分析資安警報根因，徹底解決風險。

3. 藉由通報平台系統自動比對軟體資產之弱點，以利執行軟體資產盤點作業(CPE)，落實掌握關鍵資訊系統之潛在弱點(CVE)情況。
4. 與鄰近縣市之備份、備援協力，組成堅實第一線防護陣容，當發生資通安全事件，可盡速回復服務。

十二、相關聯絡資料

機關單位	姓名	電話	E-mail
桃園市政府	詹秀峰	03-3322101#6961	10053158@mail.tycg.gov.tw
	李清吉	03-3322101#6962	10019015@mail.tycg.gov.tw
新竹市政府	林宏叡	03-5216121#340	01024@ems.hccg.gov.tw
	黃心韻	03-5216121#339	010123@ems.hccg.gov.tw
新竹縣政府	沈慧虹	03-5518101#3766	hhshen@hchg.gov.tw
	許添財	03-5518101#3771	Hsu_Tien_Tsai@hchg.gov.tw
	邸鴻文	03-5518101#3752	20034519@hchg.gov.tw
苗栗縣政府	歐聰慧	037-559748	jason@ems.miaoli.gov.tw
	謝明亨	037-559745	herryhsieh@ems.miaoli.gov.tw

附件4

政府基層機關資安主動防禦之分項計畫

臺中市政府(含彰化縣、南投縣政府)

計畫全程：112年1月至113年12月

中彰投區域縣市政府
強化政府基層機關資安防護計畫

一、 計畫緣起

（一） 政策依據：

延續 106～109 年「前瞻基礎建設計畫」，其中「數位建設」子項目一「強化政府基層機關資安防護及區域聯防」所建置之資安區域聯防機制，並依第六期「國家資通安全發展方案」(110 年至 113 年)，賡續推動政府資訊(安)向上集中，落實資源整合共享具體相關措施，期能制敵機先阻絕攻擊於邊境外，特擬訂本計畫。

（二） 待解決問題：

運用資通技術推展市政服務已屬常態，各機關單位對資訊應用的程度日益提高，從個人的資安認知與使用習慣，到整體資安能量的建構，在資訊(安)人力有限情形下，如何能提高所屬機關涵蓋面，達到一致性的防護基準，已為當前的重要課題。資訊系統為第一線面臨攻擊的切面(Attach Phase)，面對組態設定、系統弱點、存取控制不周全等問題，除造成易遭受入侵成功，又駭客使用網站後門(webshell)程式具有容易隱藏及躲避偵測等特性，也易發生網站系統遭入侵並長期攻佔而管理者未察覺等狀況，如何提昇即時的感知與應變，以及資安事件的偵測、鑑識、應變處理、情資分享等，都待我們強化運作機制及持續維運以克服此類問題。

（三） 目前環境需求分析與未來環境預測說明：

區域內縣市政府均已建置共構機房，惟限於地理位置、通訊費用及上級業務主管機關的特殊性質(如警察、衛生、地政、消防、文化局圖書館等)，造成部分所屬機關仍未納入共構機房，甚或未納入共構網路。

其次，為了提升管理效能，針對共通性系統進行整合，進一步減少各機關主機數量，經過多年來逐步推動，已建置有公文系統、電子郵件、虛擬主機服務等多項共用系統，初步落實資訊資源整合共享機制。

近來資安事件頻傳，駭客入侵成功後，將大部分主機加密，用來向

業主勒索金錢等行為氾濫，犯罪來源顯示以外國居多，相信未來也無法避免這種作為，因此，資訊資源向上集中以外，需思考完善異地備援機制，採用新一代的簽入認證機制，系統整合以集中強化資安防護，建置新一代入侵偵測系統(含防火牆)，導入弱點通報(VANS)積極辦理修補工作，建置端點監控(EDR)機制等，都是目前可預見之需求。

二、 計畫目標

本計畫以強化基層機關資安防護為核心，並參考國家發展委員會的「建構公教體系綠能資料中心計畫」、行政院國家資通安全會報的「電腦機房異地備援機制參考指引」、「行政院及所屬各機關資料中心設置作業要點」、「政府機關資訊系統弱點通報機制」(VANS) 、「導入端點監控及應變機制」(EDR)等政策方針，並評估現有資源環境，依前述環境需求分析與未來環境預測方向，展開為四個目標，分別是資訊資源向上集中、精進資安防護能量、提供實證場域—滲透測試及紅藍軍攻防演練。

（一） 資訊資源向上集中

1. 資料中心減量及網路共構共用

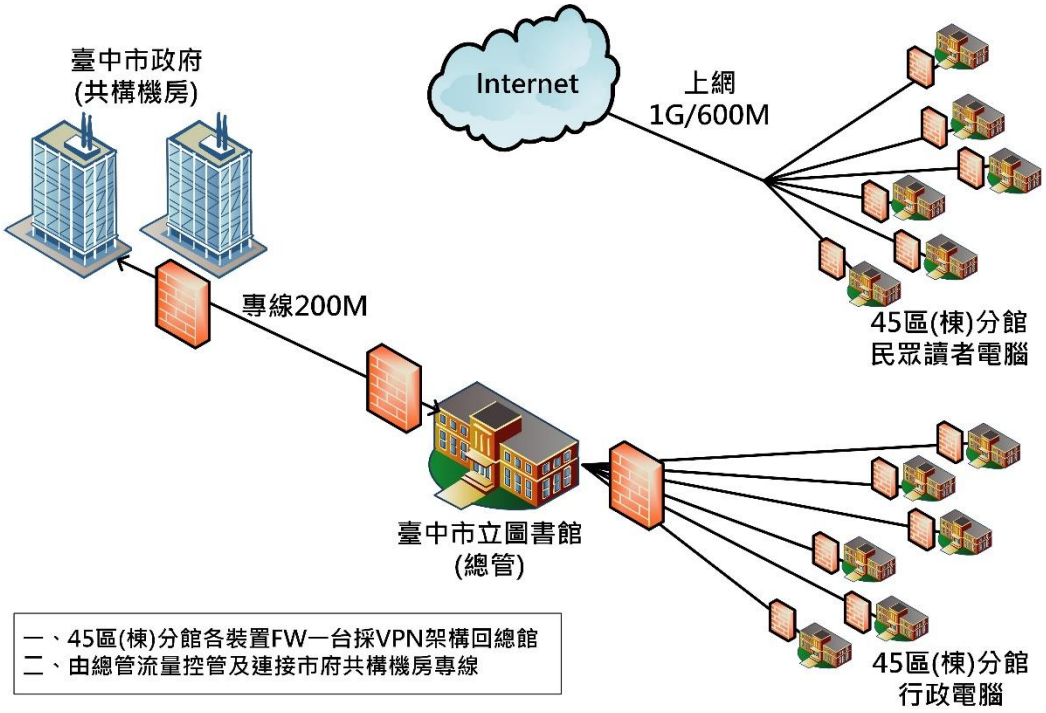
運用現行自有資料中心收容所屬機關設備，將所屬機關(含外點單位)納入共構網路達到相同資安防護等級，本計畫將審視及協調所屬機關納入前述機制，並依需求提升相關資安配套措施，包含：網路頻寬、APT 防護偵測設備、入侵偵測

系統、動態 DNS 系統等等。

臺中市政府：

收容臺中市立圖書館及所屬機關(含外點 45 個分館)資訊機房，各分館網路線路集中整併，民眾讀者上網與公務網路分離，系統主機納入市府共構機房。

提升市府共構機房核心網路資安設備收納容量，精進核心防火牆、入侵偵測系統及外部防火牆等基礎網路設施，以達到相同資安防護等級，強化網路資安整體架構。



一、 圖 1：臺中市立圖書館向上集中架構示意圖

南投縣政府：

強化南投縣政府現有資料中心資訊服務及資安防護能量，並整併南投縣政府所屬消防局、文化局網路至南投縣政府大內網架構中，由本府進行統一管理資訊流進出口，加強防護；該 2 機關個別資訊系統亦集中移置南投縣政府資料中心，且該重複之行政必要系統（如差勤、公文等系統）改以本府共用性系統取代。

2. 建置及推廣共用性系統

建置及推廣共用性系統，以集中資安人力、物力之能

量，加強檢測及防護，使得核心系統可以確實達到防護目標，將蒐集重複建置、功能性質類似項目優先納入。

彰化縣政府：

建置公所版電子郵件系統，藉由電子郵件向上集中以強化基層機關資安防護能量，落實資安法精神，並解決基層機關因電子郵件系統而需將資安責任等級升級為C級所需面臨經費及人力不足的困境，並可符合法遵及降低整體公務機關資安風險。

南投縣政府：

各單位重複之行政必要系統（如差勤、公文等系統）改以本府共用性系統取代，並新建之共用郵件系統，由南投縣政府集中賡續維運。

（二） 精進資安防護能量

1. 輔導C級機關導入「政府機關資訊系統弱點通報機制(VANS)」:

資訊安全是一種風險管理作業，如何降低可受攻擊弱點為資訊安全程序中重要且持續的工作，又參考網路攻擊狙殺鏈(Cyber Kill Chain)之攻擊七階段，如能有效降低於偵查階段之發生機會，對於資通系統弱點之主動發掘、通報及修補機制顯得更加重要，本計畫配合中央政策，將協助區域內資安責任等級C級機關導入「政府機關資安弱點通報機制」(Vulnerability Alert and Notification System, VANS)，並規劃智慧分流方式派送更新軟體進行快速部署，以因應幅員廣大、部份機關網路頻寬不足的問題。

2. 輔導B級機關導入「端點偵測及應變機制(EDR)」:

考量資通安全威脅日趨多樣，為提升資通安全責任等級B級之公務機關主動式偵測、漏洞防護、行為分析與回應之能力，宜導入端點安全防護作業，並依資通安全等級分級辦法最新增訂端點偵測及應變機制之規定（110年8月23日），協助本聯防區域B級公務機關於法規修正兩年內完成端點偵測及應變機制導入作業，及依主管機關指定方式提交偵測資

料。

（三） 提供實證場域—滲透測試及紅藍軍攻防演練：

面對當前資安發展議題與趨勢，各界均亟需資安人才，透過實戰演練，可以有效增進彼此需求的了解，有助啟發學術界進一步了解目前資安待解決問題，運用政府資源(料)進行研究，促進校園端對於資安人才培育的訓練與課程規劃，同時藉由演練分享交流機會，提昇學子對於資安職涯認知，提高畢業後投入資安產業之意願。

1. 為提升基層人員資安技術能量符合資安法資安人力訓練要求，舉辦資安專業證照及資安職能提升訓練 20 人次。
2. 資安攻防職能訓練及實作平台 30 人次 2 天。
3. 辦理紅藍隊演練，由本府提供適當攻防場域系統規劃紅隊(業界滲透測試團隊及學術單位組隊)與藍隊(市府及現有資安委外廠商)進行黑箱/灰箱攻防測試，預計整體演練時間為 3 完整天。
4. 辦理中部地區滲透攻防資安技術交流會議每年 40 人次

三、 計畫內容與實施策略

（一） 資訊資源向上集中

1. 資料中心減量及網路共構共用

臺中市政府：

(1) 圖書總館系統向上集中：

進行臺中市立圖書館資訊機房向上集中至本府資料中心，收容包含：志工管理系統、場地管理系統、館員知識管理平台系統、推播系統、公用電腦管理系統及公用電腦保護系統等相關系統。在共用資料中心建置約 50 台虛擬機資源，並辦理資訊系統轉移、虛擬機轉移、管理平台建置、資料備份管理、系統效能監控、系統異常告警、系統軟體授權、系統日誌管理等工作。

(2) 圖書總館整併分館網路線路：

配合機房整併，臺中市立圖書館及所屬 45 個分館須配套納入共構網路，汰換各分館原各自申請之 GSN 或中華電信光世代寬頻網路，改統一申辦雙路由混合型網路線路，並重新進行各分館網路架構及線路調整，以符合線路線上集中之環境條件。公務上網流量採 VPN 架構收攏連線回總館，再由總館擔任中繼站管控分流，並透過獨立專線連接回本府；其他外部網路出口流量則由電信業者機房端直接出去，並統一由資安設備加以防護。透過網路向上集中以強化核心網路管理及資安防護效益。

(3) 精進市府共構機房資安網路設備：

因應臺中市立圖書館資訊機房網路線路集中收納、市府共構網路流量使用量增加，預期將超過核心防火牆及入侵偵測系統等設備威脅防護輸送量使用上限 2.4Gbps，爰配套辦理市府核心網路設備升級汰換，包含市府網路核心防火牆 2 台(HA)、入侵偵測系統 2 台(HA)及外部防火牆設備 2 台(HA)等設備，預期可提升威脅防護輸送量使用上限為 7.2Gpbs、出口頻寬處理能力可由原 1Gbps 提升至 2.5Gbps 以上，以優化核心網路架構、確保市府共構網路服務品質。

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	臺中市立圖書館總館暨45個分館	臺中市立圖書館暨所屬44個分館VPN線路汰換建置
	主機向上集中及系統整併	臺中市立圖書館總館	整併收容臺中市立圖書館資訊機房至本府資料中心，在共用資料中心建置約50台虛擬機資源，並辦理資訊系統轉移相關作業。
	精進市府共構網路設備	臺中市政府市政共構機房	精進市府共構網路核心防火牆、入侵偵測系統及外部防火牆等基礎網路設施

南投縣政府：

配合中央政府減少資料中心，資訊資源向上集中之政策，本計畫將就資安防護相對薄弱，外點單位多且距離遠之南投縣政府文化局、南投縣政府消防局進行資訊資源向上集中之施作，並將該些單位重複之行政必要系統改以本府共用性系統取代，以及將該2機關個別專用資訊系統集中移置本府機房，再由本府進行統一管理資訊流進出口，加強防護。以此為藍本，日後將可視本府經費資源狀況，逐一將資安防護較薄弱之所屬機關及公所逐一納入。

2. 建置及推廣共用系統

彰化縣政府：

彰化縣建構集中式電子郵件系統，提供26個鄉鎮市公所使用，以降低基層機關所面臨之資安威脅。

南投縣政府：

南投縣將強化行政必要系統之功能及效能，如共構式全球資訊網網頁服務、電子郵件、差勤、公文等系統，並舉辦相應教育訓練，俾提供參與本案向上集中機關提供足夠服務能量及誘因，使同仁將日常公務上所需資訊服務，順利移轉至本府提供系統，達成系統共用之目標。

(二) 精進資安防護能量

1. 導入「政府機關資訊系統弱點通報機制(VANS)」

行政院國家資通安全會報技術服務中心推廣「政府機關資

安弱點通報機制」(簡稱 VANS 系統)，藉由通報平台系統自動比對軟體資產之弱點，以利執行軟體資產盤點作業(CPE)，落實掌握關鍵資訊系統之潛在弱點(CVE)情況；本計畫將透過專管系統建置，進行軟體資產蒐集、盤點、上傳及後續配套作業，協助區域內縣市所屬 14 個資安責任等級 B 級機關導入，並可確保用戶端電腦中軟體資產因應緊急重大弱點更新的需求，可以智慧分流方式，降低受 VPN 頻寬限制影響，達到快速派送更新需求，相關工作內容如下：

- 辦理「政府機關資訊系統弱點通報機制」(VANS)說明會議。
- 輔導聯防區域內三縣市共 71 個 C 級機關(臺中:39 個，7,000 台設備、彰化:19 個，3,000 台設備、南投:13 個，1,300 台設備)加入 VANS 通報機制，並達 100%通報率。
- 提供 VANS 通報儀表板彙整通報概況。
- 針對緊急重大弱點軟體安全性更新或修補，提供管理工具盤點用戶端電腦即時更新狀態，並確認是否需要排程進行後續更新作業。
- 軟體派送更新須具備智慧分流機制，以加速轄區內軟體下載效率，透過同網段內設備與設備相互連接特性並啟用安全檔案傳輸機制，並顯示整體派送下載路線拓樸圖供管理者檢視調整。

2. 輔導 B 級機關導入「端點偵測及應變機制(EDR)」：

為協助導入端點偵測及應變機制(EDR)，通知本聯防區域 B 級機關調查需求數量，辦理導入說明會，並優先評估採用國內自主研發之 EDR 品牌，以扶植國內資安發展。預計於 112 年至 113 年分別完成導入端點偵測及應變機制(EDR)及納入 SOC 監控，並依資通安全管理法主管機關指定方式提交端點偵測及應變機制(EDR)偵測資料。

本聯防區域預計導入 B 級機關及數量為：臺中市(8 個機關，5,000 台設備)、彰化縣(4 個機關，500 台設備)、南投縣(2 個機關，1,800 台設備)。

（三） 提供實證場域—滲透測試及紅藍軍攻防演練：

106 至 109 年中彰投資安培力以區域治理概念，結合區域內政府資訊(安)管理人員及區域內大專院校師生，提供實作培力與管理面養成訓練，取得資安專業技能及知識。

為培育國內資安人才，並且滿足業界對於資安人才之強勁需求，除延續辦理資安鑑識營隊以外，也開放實驗場域，並規劃結合行政院國家資通安全會報技術服務中心規劃之資安職能訓練發展藍圖，工作內容如下：

1. 每年辦理中部地區滲透攻防資安技術交流會議 2 場次，會議內含括：專題演講、近期中彰投縣市政府區域聯防概況、國內或國際重大資安事件解析、資安事件個案研討等。
2. 為提升基層人員資安技術能量符合資安法資安人力訓練要求，舉辦資安專業證照及資安職能提升訓練 20 人次。

基層機關多數是研考人員兼辦及非資訊領域相關背景兼辦資安工作，惟行政院及各級機關持續辦理相關專長訓練，已收初步成效，部分人員也有意願從事專職資安業務，顯見持續訓練的重要性。

因此，本案將持續規劃以符合資安法資安職能要求之資安治理與管理相關證照課程提升基層人員資安職能，目標是能夠傳達資安責任等級應辦事項內容，協助同仁更深入了解及落實資安業務。

3. 資安攻防職能訓練及實作平台 30 人次

近年在資安意識抬頭及資通安全法的推動下，大多數同仁對於資訊安全的防護概念有逐漸提升，單位均開始導入 ISO 27001（ISMS）並取得認證，以維護資訊安全的基礎管理措施。

然而在面對真正的網路威脅攻擊時，大多數取得 ISMS 證照或資訊人員可能因不了解攻擊手法，也沒有足夠的應變經驗而束手無策。課程將設計「基礎攻擊訓練課程」及「基礎應變分析課程」兩種，期望藉由這樣的平台訓練，精進專責人員的演習測試與實戰能力，強化資安事件處置能力，以培

養出更多在地化的資訊資安人員。

4. 辦理大專院校及政府機關資安專責人員鑑識營隊，各一場次，每場次兩天，除專題演講以外，提供教學案例及平台，實機進行演練及競賽，至少 30 人次。

加強學術界及政府機關資安人員接觸資安實務的經驗，加強學生對於未來職場的準備以及資安人員實際應變資安案例，規劃舉辦資安鑑識營隊，讓參與課程學員從實務案例做中學。

規劃課程大綱
1. 資安事件實例說明 2. 如何自行定位惡意程式 3. 受駭主機惡意程式定位實作(VM &Demo) 4. 惡意程式檢測工具說明與實作(Demo) 5. 駭客內網入侵手法說明及免費個人電腦安全檢測工具介紹

5. 辦理中部地區滲透攻防資安技術交流會議每年 40 人次，會議內容涵括：專題演講、近期中彰投縣市政府區域聯防概況、國內或國際重大資安事件解析、資安事件個案研討等。

四、 實施範圍

本案實施範圍為主要為臺中市政府及所屬機關、彰化縣政府及所屬機關、彰化縣各鄉鎮市公所、南投縣政府及所屬機關、南投縣各鄉鎮市公所，資安情資交流分享並將邀請有意願加入之中部地區中央機關、教育、醫療、金融、科技等機關單位。

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

（一） 臺中市政府

年度	項次	關鍵績效指標	目標值

112	1	縮減實體主機營運累計數量(單位:台)。	收容至 25 個虛擬機
	2	累計整併線路數量(單位:條)。	臺中市立圖書館各分館之 20 條線路。
	3	C 級機關導入政府機關資安弱點通報機制(VANS)導入率(%)	100%(導入 C 級機關個數/C 級機關總數,C 級機關總數 39 個)
	4	B級機關導入「端點偵測及應變機制(EDR)」第一期導入率(%)	100%(導入 B 級機關個數/第一期 B 級機關總數 4 個，第一期 B 級機關總數 4 個)
	5	資安人才培訓人次 國際證照訓練 職能訓練	1. 基層人員資安證照取得 20 人/年。 2. 資安攻防職能訓練及實作平台 30 人次/年
	6	紅藍隊演練	每年辦理資安實證場域(紅藍隊/年)一案,並產出檢討報告
	7	鑑識營隊 技術交流會議	資安鑑識營隊 2 場次/年 技術交流會議參與 40 人次/年
113	1	小型機房減少數(個)	臺中市立圖書館 1 個總館機房
	2	縮減實體主機營運累計數量(單位:台)。	收容至 25 個虛擬機
	3	累計整併線路數量(單位:條)。	臺中市立圖書館各分館之 25 條線路。
	4	B級機關導入「端點偵測及應變機制(EDR)」第二期導入率(%)	100%(導入 B 級機關個數/第二期 B 級機關總數，第二期 B 級機關總數 4 個)
	5	EDR 資料提交機制完成率 (%)	100%(導入 B 級機關個數/B 級機關總數,B 級機關總數 8 個)
	6	資安人才培訓人次 國際證照訓練 職能訓練	1. 基層人員資安證照取得 20 人/年 2. 資安攻防職能訓練及實作平台 30 人次/年
	7	紅藍隊演練	每年辦理資安實證場域(紅藍隊/年)一案,並產出檢討報告
	8	鑑識營隊 技術交流會議	資安鑑識營隊 2 場次/年 技術交流會議參與 40 人次/年

（二） 彰化縣政府

年度	項次	關鍵績效指標	目標值
112	1	C 級機關導入政府機關資安弱點通報機制(VANS)導入率(%)	100%

		(導入 C 級機關個數/C 級機關總數)	
	2	B 級機關導入「端點偵測及應變機制(EDR)」導入率（%）(導入 B 級機關個數/B 級機關總數，B 級機關總數 4)	100%
113	3	B 級機關 EDR 資料提交機制完成率(%)(完成提交 B 級機關個數/B 級機關總數，B 級機關總數 4)	100%

（三） 南投縣政府

年度	項次	關鍵績效指標	目標值
112	1	小型機房減少數(個)	1
	2	縮減實體主機營運累計數量(單位:台)。	5
	3	累計整併線路數量(單位:條)。	14
	4	C 級機關導入政府機關資安弱點通報機制(VANS)導入率(%)	100%(導 C 級機關個數/C 級機關總數，C 級機關總數 13 個)
113	1	小型機房減少數(個)	1
	2	縮減實體主機營運累計數量(單位:台)。	5
	3	累計整併線路數量(單位:條)。	23
	4	B 級機關導入「端點偵測及應變機制(EDR)」導入率（%）	100%(導入 B 級機關個數/B 級機關總數，B 級機關總數 2 個)
	5	EDR 資料提交機制完成率（%）	100%(導入 B 級機關個數/B 級機關總數，B 級機關總數 2 個)

七、 持續營運評估

對於計畫補助以後，持續維運的具體作為及評估如下：

（一） 資訊資源向上集中：

1. 經由本計畫採購之網路設備及系統，於計畫執行完畢後，網路費用及系統維運費用，可由文化局、消防局等整併進來的

機關原資訊預算，併入南投縣政府資訊預算賡續維護，持續營運。

2. 差勤、公文等共用系統原已集中維運，因集中而新建之共用郵件系統將由南投縣政府集中賡續維運。
3. 彰化縣公所版共構式電子郵件系統由彰化政府集中維護，持續營運。
4. 臺中市立圖書館向上集中後相關維運經費如下表：

績效目標	項次	工作目標	後續維運服務模式	後續維運經費評估
資訊資源向上集中	1	整併網路線路	線路費及設備維護	由臺中市政府圖書館每年編列預算維護： 網路線路租用費用，每年約3,000仟元
	2	主機向上集中及系統整併	設備及系統維護	由臺中市政府圖書館每年編列預算維護： 共用資料中心系統維運50個虛擬機，設備及系統維運費約建置經費15%，約750仟元。
	3	精進市府共構網路設備	設備維護	由臺中市政府資訊中心每年編列預算維護： 設備維運費約建置經費15%，約2,550仟元

（二） 精進資安防護能量：

「政府機關資訊系統弱點通報機制(VANS)」及「端點監測及應變機制(EDR)」預計納入應辦事項之一，將由區域內縣市政府統一建置維運，B、C級機關配合使用操作，可減省經費及人力，後續將依法遵要求編列運算持續運作。

（三） 資安人才培訓：

透過資安人才培訓，分享多元資安情報，提升基層資安防禦，進行資安人才培力，以達落實技術、蒐集數據、優化商業模式及提供創新服務等效益，人才接軌資安發展需求。

八、 經費明細概算

（一） 臺中市政府

單位：新臺幣元

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	整併網路線路。	4,949,214	2,248,314	1. 辦理臺中市立圖書館及所屬 20 個分館納入共構網路。 2. 辦理臺中市立圖書館及所屬 20 個分館網路線路架構重新佈線及調整，以符合網路集中化環境。 3. 建置總館收容分館網路線路專用之交換器及防火牆(HA 架構)	1
	2		主機向上集中及系統整併。	400,000	1,100,000	1. 整併臺中市立圖書館資訊機房至本府中心 2. 建置本府資料中心 25 個虛擬機資源，包含：志工管理系統、場地管理系統、館員知識管理	2

						平台系統、推播系統及公用電腦管理系統、公用電腦保護系統等等。辦理資訊系統轉移、虛擬機轉移、管理平台建置、資料備份管理、系統效能監控、系統異常告警、系統軟體授權、系統日誌管理等工作。	
	3		精進市府共構網路設備-核心防火牆。	740,000	4,500,000	汰換核心防火牆2台，預期威脅防護輸送量使用上限由原2.4Gbp提升為7.2Gpbs，並互為備援，以確保網路服務高可靠度及提升市府核心網路收納能力。	3
	4		精進市府共構網路設備-入侵偵測系統。	720,000	6,000,000	汰換入侵偵測系統2台，預期威脅防護輸送量使用上限由原2.4Gbp提升為7.2Gpbs，並互為備援，以確保網路服務高可靠度及提升市府核心網路收納能力。	4
	5		精進市府共構網路設備-外部防火牆。	100,000	800,000	汰換外部防火牆2台，預期出口	5

						頻寬處理能力可由原 1Gbps 提升至 2.5Gbps 以上，並互為備援，以確保網路服務高可靠度及提升市府核心網路收納能力。	
	6	精進資安防護能量	導入「政府機關資訊系統弱點通報機制」(VANS)。	7,000,000	-	1.機關 VANS 建置與輔導導入、測試及派送功能驗證作業(39 個機關，7000 台設備)。 2.智慧分流軟體派送配套機制	6
	7		導入「端點偵測及應變機制(EDR)」(第一期)。	9,000,000	-	本聯防區域預計導入 B 級機關及數量為：臺中市(8 個機關共 5000 台，本年度先導入 2500 台設備)。	7
	8	推動滲透測試及紅藍軍攻防演練	基層人員資安證照取得 20 人/年。	900,000	-	資安專業證照及資安職能提升訓練 20 人次/年。	8
	9		資安攻防職能訓練及實作平台 30 人次/年。	540,000	-	資安攻防職能訓練及實作平台 30 人次/年。	9
	10		資安攻防實證場域(紅藍隊)。	720,000	-	規劃紅隊(業界滲透測試團隊及學術單位組隊)與藍隊(市府及現有資安委外廠商)進行黑箱/灰箱攻防測試，並產出檢討報告/每年一次。	10
	11		資安鑑識營隊 2 場	720,000	-	資安攻防鑑識營隊(30 人/每場	11

			次/年。			次)，每年2場次。	
	12		技術交流會議參與40人次/年。	235,000	-	技術交流會議參與40人次/年。	12
小　　計				26,024,214	14,648,314		
合　　計					40,672,528		

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	13	資訊資源向上集中	整併網路線路。	5,755,071	3,045,000	1.辦理臺中市立圖書館及所屬25個分館納入共構網路。 2.辦理臺中市立圖書館及所屬25個分館網路線路架構重新佈線及調整，以符合網路集中化環境。	
	14		主機向上集中及系統整併。	834,000	1,522,500	1.整併臺中市立圖書館資訊機房至本府中心。 2.續收容圖書館25個虛擬機資源，包含：志	

						工管理系統、場地管理系統、館員知識管理平台系統、推播系統及公用電腦管理系統、公用電腦保護系統等等。辦理資訊系統轉移、虛擬機轉移、管理平台建置、資料備份管理、系統效能監控、系統異常告警、系統軟體授權、系統日誌管理等工作。	
	15	精進資安防護能量	完成資通安全管理法主管機關指定方式提交端點偵測及應變機制(EDR)偵測資料(第二期)。	9,000,000	-	本聯防區域預計導入B級機關及數量為：臺中市(8個機關共5000台，本年度再導入2500台設備)，於113年納入SOC監控，依資通安全管理法主管機關指定方式提交端點偵測及應變機制(EDR)偵測資料。	
	16	資安人才培訓	基層人員資安證照取得20人/年。	900,000	-	資安專業證照及資安職能提升訓	

						練 20 人次/年。	
	17		資安攻防職能訓練及實作平台 30 人次/年。	540,000	-	資安攻防職能訓練及實作平台 30 人次/年。	
	18		資安攻防實證場域(紅藍隊)。	720,000	-	規劃紅隊(業界滲透測試團隊及學術單位組隊)與藍隊(市府及現有資安委外廠商)進行黑箱/灰箱攻防測試，並產出檢討報告/每年一次。	
	19		資安鑑識營隊 2 場次/年。	720,000	-	資安攻防鑑識營隊(30 人/每場次)，每年 2 場次。	
	20		技術交流會議參與 40 人次/年。	235,000	-	技術交流會議參與 40 人次/年。	
小　　計				18,704,071	4,567,500		
合　　計					23,271,571		

（二） 彰化縣政府

單位：新臺幣元

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	精進資安防護能量	導入「政府機關資訊系統弱點通報機制」(VANS)。	8,400,000	575,000	C 級機關 VANS 導入(衛生局、消防局、環保局、文化局、各地政所	1

						及鄉鎮公所）及B級機關教育網路中心擴大推廣導入。	
	2	精進資安防護能量	導入「端點偵測及應變機制(EDR)」。	2,310,000	0	本府、警察局、地方稅務局及教育網路中心導入EDR系統。	2
	3	資訊資源向上集中	導入電子郵件系統。	1,688,750	4,751,250	導入電子郵件系統供各鄉鎮市公所使用。	3
小　　計				12,398,750	5,326,250		
合　　計				17,725,000			

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	精進資安防護能量	提交端點偵測及應變機制(EDR)偵測資料。	4,160,000	0	本府、警察局、地方稅務局及教育網路中心持續推廣導入範圍並提交端點偵測及應變機制(EDR)偵測資料。	1
小　　計				4,160,000	0		
合　　計				4,160,000			

（三） 南投縣政府

單位：新臺幣元

年度	項	工作	工作內容	所需經費	績效	優

	次	項目		經常門	資本門	目標	先次序
112	1	資訊向上集中	進行南投縣政府消防局及文化局之資訊向上集中工程。	2,693,000	23,718,375	累積減少 1 資訊機房。	1
	2	精進資安防護能量	導入政府機關資訊系統弱點通報機制(VANS)至本府 C 級機關。	1,948,250	0	完成所屬資安責任等級 C 級機關政府機關資訊系統弱點通報機制(VANS)導入。	2
小　　計				4,641,250	23,718,375		
合　　計					28,359,625		

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	資訊向上集中	進行南投縣政府消防局及文化局之資訊向上集中工程。	8,076,000	10,767,337	累積減少 2 資訊機房。	1
	2	精進資安防護能量	本府暨所屬資安責任等級 B 級以上機關導入端點偵測及應變機制（EDR)。	7,529,900	0	完成本府暨所屬資安責任等級 B 級機關導入 EDR 系統，於 113 年納入 SOC 監控，依資通安全管理法主管機關指定方式提交端點偵測及應變機制(EDR)偵測資料。	
小　　計				15,605,900	10,767,337		

合　　計	26,373,237		

九、 經費補助表

單位：新臺幣元

（一） 臺中市政府

年度	總經費	補助比例	其他基金或補助款	地方政府自籌款	行政院補助款
112	40,672,528	0.7	0	12,201,758	28,470,770
113	23,271,571	0.7	0	6,981,471	16,290,100

（二） 彰化縣政府

年度	總經費	補助比例	其他基金或補助款	地方政府自籌款	行政院補助款
112	17,725,000	0.8	0	3,545,000	14,180,000
113	4,160,000	0.8	0	832,000	3,328,000

（三） 南投縣政府

年度	總經費	補助比例	其他基金或補助款	地方政府自籌款	行政院補助款
112	28,359,625	0.8	0	5,671,925	22,687,700
113	26,373,237	0.8	0	5,263,897	21,098,590

（四） 中彰投經費彙整總表

單位：新臺幣元

年度	臺中市政府	彰化縣政府	南投縣政府
112	40,672,528	17,725,000	28,359,625
113	23,271,571	4,160,000	26,373,237

十、 預定進度

（一） 臺中市政府

時程	累計預定	累計預定支	關鍵查核點

	進度(%)	用費用(元)	
112/12	50%	40,672,528	1.完成收容圖書館25個虛擬機資源。 2.完成臺中市立圖書館所屬20個分館，網路線路架構重新佈線及線路整併作業，並建置總館收容分館網路線路專用之交換器及防火牆(HA架構)(第一期) 3.完成提升建置市府共構網路核心防火牆、入侵偵測系統及外部防火牆等配套基礎網路設施。 4.C級機關39個VANS導入 5.B級機關導入EDR第一期 6.資安相關訓練、營隊及紅藍隊演練、技術交流
113/12	100%	63,944,099	1.完成臺中市立圖書館所屬25個分館，網路線路架構重新佈線及線路整併作業(第二期)，整併圖書館資訊機房至本府中心後減少機房數1個 2.續收容圖書館25個虛擬機資源，並辦理資訊系統轉移、虛擬機轉移、管理平台建置、資料備份管理、系統效能監控、系統異常告警、系統軟體授權、系統日誌管理等工作。 3.B級機關導入EDR第二期，並完成資料提交機制 4.資安相關訓練、營隊及紅藍隊演練、技術交流

（二） 彰化縣政府

年度	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
112	30%	5,317,500	1.資安責任等級C級機關完成VANS採購 2.資安責任等級B級機關完成EDR採購 3.本府完成公所版電子郵件系統採購
112	100%	17,725,000	4.資安責任等級C級機關完成VANS導入 5.資安責任等級B級機關完成EDR導入 6.本府完成公所版電子郵件系統導入

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
113	100%	4,160,000	本府、警察局、地方稅務局及教育網路中心完成提交端點偵測及應變機制(EDR)偵測資料

（三） 南投縣政府

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
112/12	52%	28,359,625	1.整併網路線路 2.強化資訊中心機房服務能量 3.移動部分資訊系統
113/12	100%	54,732,862	1.購買軟體授權 2.移動所有資訊系統 3.B 級機關導入 EDR

十一、 預期效益

資通安全是台灣發展數位經濟跟數位國土的基礎，由於我國政經情勢特殊，除了面對全球複雜多元的資通訊變革，還需面對較其他國家更為險峻的資通訊安全威脅，故持續落實精進各項資通訊安全防護工作實屬必要。中彰投三縣市政府透過區域聯防共享資源的規劃，落實於中部地區建立安全資安環境，完備資安防護管理，分享多元資安情報，提升基層資安防禦，透過資安人才培力，使人才接軌資安發展需求。

本計畫完成後，可順應數位經濟到來之際，可確保中彰投同步提升應變能量，完成重要之數位建設，且可以完整地達成下列目標：

（一） 配合整併收容臺中市立圖書館及所屬機關(含外點 45 個分館)資訊機房，並辦理網路線路集中，納入共構網路統一管理，辦理提升市府核心網路收納能力，精進核心防火牆、入侵偵測系統及外部防火牆等基礎網路設施，以達到相同資安防護等級，強化網路資安整體架構。

（二） 完成試作同質性系統向上集中，加入機關僅需負責文字內容更

新，不需維護網站硬體及資安設備，可與縣府網路資安硬體設備共用，避免駭客攻擊、資安修復等問題，省卻每年硬體、軟體及資安維護費。

（三） 有助於本區南投縣政府就資訊向上集中之國家政策，建立明確目標，亦可提供該些納入向上集中規劃案之機關，日後資訊規劃之重要參考依據。

（四） 建立資訊系統弱點通報系統及對應機制，可以提升廣泛端點之弱點修補作業，有效提升安全程度，減少駭客利用系統漏洞進行惡意攻擊的風險，亦降低外點單位被利用於跳板攻擊的可能。

（五） 推動滲透測試及紅藍軍攻防演練：

為了能夠於在地資安長遠發展能夠帶動建立一個良性循環，我們已於先期前瞻計畫埋下一個資安的希望種子，希望透過市府持續發動資安實作場域及基層機關資安人才培訓讓此種子持續發芽茁壯，並養成資安人才深化與回饋組織，並從資安技術產學實習過程中鼓勵與推薦，進一步給讓在地資安廠商可以有人材選用及晉用，選材於鄉里，回饋於鄉里、最後服務於鄉里。

（六） C 級機關完成建立弱點通報機制，使機關可掌握資訊設備弱點的全貌，調配資源進行更新，以確保重要資訊設備安全。

（七） B 級機關完成端點偵測及應變機制(EDR)，採系統行為分析方式進行端點威脅偵測，可透由 AI 分析自動關聯資安事件發生之主要原因、軌跡及執行時間序，加速端點採證及資安鑑識作業效率，並可依主管機關指定方式提交偵測資料。

十二、相關聯絡資料

機關單位	姓名	電話	E-mail
臺中市政府資訊中心	張碧顯	04-22289111 #22301	ps491@taichung.gov.tw
臺中市政府資訊中心	林釗湧	04-22289111 #22208	imc16602@taichung.gov.tw
彰化縣政府計畫處	許宏基	04-7531351	a230400@email.chcg.gov.tw

彰化縣政府計畫處	吳彥懿	04-7531353	a230412@email.chcg.gov.tw
南投縣政府計畫處	周湧裕	049-2245361	ian@nantou.gov.tw
南投縣政府計畫處	賴義翔	049-2245361	davis20403@nantou.gov.tw

附件5

政府基層機關資安主動防禦之分項計畫

臺南市政府(含嘉義市、嘉義縣、雲林縣政府)

計畫全程：112年1月至113年12月

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

1. 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。

2. 計畫目標

（一）臺南市政府

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。

1. 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。

2. 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。

3. 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。

（二）嘉義市政府

1. 推動資訊資源向上集中，資料中心環控智慧化。

2. 精進地方政府資安防護能量。

（三）嘉義縣政府

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「強化政府基層機關資安防護能力」為基礎，以期達成「安全可信賴之資訊資源集中共享環境」之願景。

1. 資訊資源向上集中：建置及推廣共用性系統並建構系統安全維運通道。
2. 精進資安防護能量：導入 9 個 C 級機關 VANS、3 個 B 級機關 EDR。
3. 推動滲透測試及紅藍軍攻防演練：辦理資安檢測協助本縣改善資安防護。

（四）雲林縣政府

本計畫規劃以「資訊資源集中整併 (Resource Consolidation)」及「資訊服務共享 (Shared Services)」為兩大主軸，並以「精進資安主動防禦能力」為基礎，以期建構安全可信賴之資訊共享環境。

1. 建置共用資料中心，成立專案輔導團隊

   整併線路集中網路出口。公所機房減量，將資源集中至縣政府，公所透過 VPN 連線至行政系統。預計 112 年、113 年各執行 2 個公所，辦理資訊系統移轉作業每年 2 個系統以上。
2. 佈署基層端點防禦，精進資安防護能量

   (1) 資安管理作業電子化、自動化。

   (2) 35 個 C 級機關導入 VANS，3 個 B 級機關導入 EDR。

   (3) 統計資料圖像化，提供提前佈署、智慧分析決策，提升整體資安防護能量。
3. 推動滲透測試及紅藍軍攻防演練

   辦理資通安全健診，包括本府及鄉鎮市公所等機關，計 1,800 台以上個人電腦和資訊系統。

3. 計畫內容與實施策略

（一） 臺南市政府

1. 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：

A. 整併本市所屬 6 個外部單位資訊機房至本府資料中心。

B. 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。

C. 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。

2. 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。

3. 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。

（二） 嘉義市政府

1. 推動資訊資源向上集中

資料中心環控智慧化：

如何強化實體與環境安全，是資安工作重要的一環，也是每年資安稽核重要項目，為了持續精進資訊系統及資源之向上集中，強化系統可用性，將針對資料中心機房實體環境監控重新進行規劃與設計，包含檢視整體門禁系統、電力(含不斷

電系統)、空調、消防等設備之控制，進行介接可行性與必要性評估，並於介接中央環控系統後，強化進出人員管制措施，以及進行雲端運算強化資源擴充

2. 精進資安防護能量

(1) 建立C級機關弱點掃描檢測系統(VANS):

依據「資通安全責任等級分級辦法」規定應辦事項，除完善本府暨所屬B級機關外，更針對本府C級機關持續建立終端資產管理系統，提供所屬機關的個人電腦及筆記型電腦所安裝之軟、硬體進行定期的盤查與控管，並提供異常警示通知，能夠迅速地提供調查與處理之必要資訊，以及配合行政院推動政府資訊系統弱點通報機制(VANS)，具備支援資產正規化的轉換系統，可大幅降低軟體資產盤點與正規化作業所需耗費之時間與心力。

(2) 強化遠端連線監控及稽核作業:

近年供應鏈造成的問題已成為新興之資訊安全議題，除了依據行政院建議強化遠端連線管理外，將再針對重點系統進行連線稽核機制優化，透過可監控之稽核管理，將申請連線之使用者針對其系統性質及操作行為，建立規則化之管理，並留下相關紀錄，以進行後續追蹤管制措施。

（三） 嘉義縣政府

本計畫以「資訊資源向上集中」為目標主軸，沿續前期「強化政府基層機關資安防護計畫」精神，建置並推廣共用性系統，完善共用資料中心，並透過「精進資安服務能量」各項作業強化共構機房資安防護能力，以降低基層機關承擔獨自連網之資安風險，全面性提昇本縣資訊安全防護能力，規劃本縣「資安整合共構服務架構圖」，實施範圍如下：

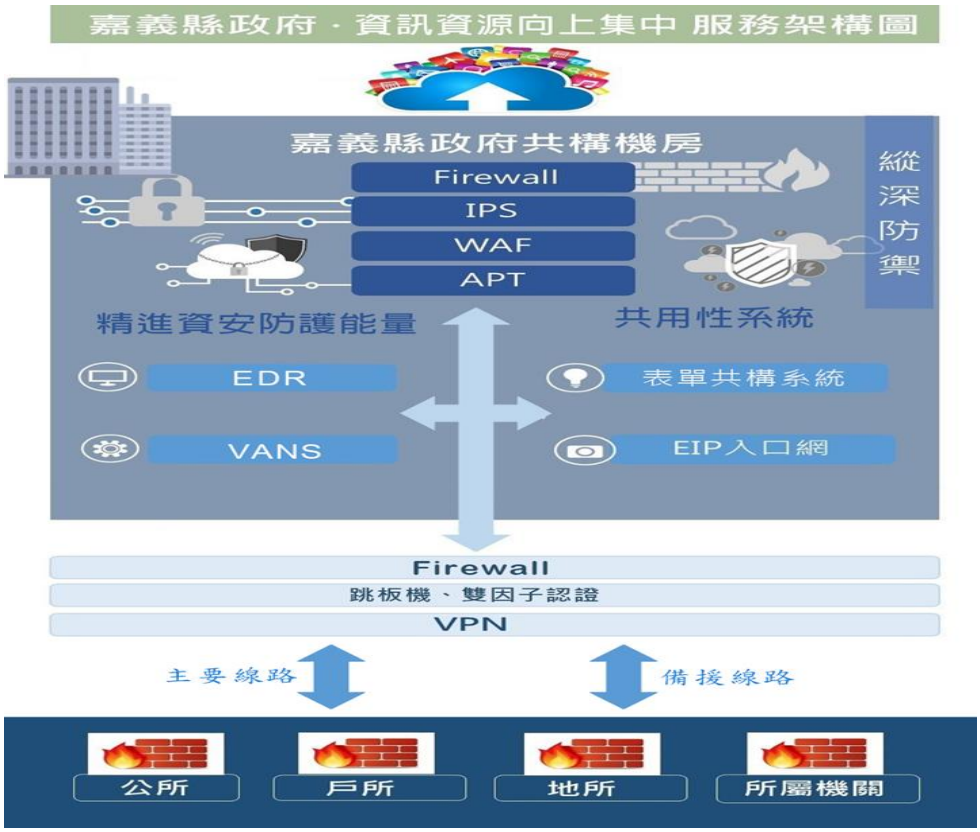


圖 1：服務架構圖

4. 資訊資源向上集中

(1) 建置及推廣共用性系統：

建置「EIP 入口網站」及「表單共構系統」，推廣至本縣所屬各機關、鄉鎮市公所及代表會使用。

A. 建置「EIP 入口網站」

本府於民國 92 年建置之行政資訊入口網系統，提供本府使用者使用單一簽入公文系統、人事差勤、便民服務、一般公告、活動看板、資訊發佈平台、檔案分享傳輸、行事曆等服務。

因系統之原開發軟體技術及設備老舊，無法更新或改版符合相關資訊安全要求，更重要的是為推廣本府 11 個所屬機關及 18 鄉鎮市公所使用，需進行系統更換及設備更新等來達到功能及資訊安全的要求。

B. 建置「表單共構系統」

為有效管理本縣共用性系統及落實資通安全管理制度，透過共構表單設計整合本府各局處暨所屬機關、18 個鄉鎮

市公所，提供電子化表單簽核作業，將資訊化繁為簡，減少文件及紙本表單簽核時間，強化資訊宣導速度並提升管理效率。

(2) 建構系統安全維運通道

建置「主機代理連線、稽核及特權用戶管理機制」、「雙因子認證」等資安基礎建設，加強遠端存取控制機制，達到資安統一管理。

1. 建置「主機代理連線、稽核及特權用戶管理機制」

因應伺服器資源向上集中，遠端桌面連線維護需求大量增加，新增跳板機制以利資訊安全控管，並同時降低中毒橫向擴散之風險，有效建立損害管制防線。

2. 建置「雙因子認證」

近期的資安防護及推動策略係採用零信任(Zero Trust)防護架構，內網應視同外網，且需妥善管理委外廠商，為鞏固本府共用性系統的第一道防線，建構雙因子認證以強化登入系統之安全性，利用多樣化驗證機制模式，確認遠端登入者身分，避免外部惡意侵入。

5. 精進資安防護能量

(1) 推動導入資訊系統弱點通報機制 VANS（9 個 C 級機關）。

(2) 推動導入建立端點威脅偵測及應變機制 EDR（3 個 B 級機關）。

6. 推動滲透測試及紅藍軍攻防演練

辦理 900 台個人電腦及 30 個系統資安檢測。

（四） 雲林縣政府

1. 推動資訊資源向上集中

(1) 整併線路集中網路出口

建置全縣共構機房及共構系統，辦理提升本府出口網路頻寬，精進防火牆、入侵防護系統等網路與資安基礎建設，及進行本府基層機關（所屬部分機關：4 個鄉鎮市公所）VPN 線路建置、收容及監控服務，提升整體資訊資源使用效率及

資安防護能量。

(2) 建置 Windows Server Update Services (WSUS)

配合每月微軟發布的更新程式，將發現的安全漏洞盡快更新及補強，減少駭客可利用的機會。建置 Windows Server Update Services (WSUS)，採集中管理方式，管控所有個人電腦派送更新時間，並擇部分單位先測試更新後之狀況，如無異常狀況，再大量分批佈署，以減少使用者操作系統時之非預期情況，完成安全漏洞之更新。

(3) 建置日誌 (Log) 蒐集系統

配合所屬機關網路向上集中至縣府，在落實資訊資源整合共享的同時，為強化各路線路管理以及網路安全防禦架構，需加強流量管理平台網路流量之可視性。建置 Log 蒐集系統，把縣府現有資安設備（如防火牆、IPS 及 WAF）、網路設備（如 switch）及重要主機設備（如公文系統、電子郵件及全球資訊網站等）所產出的 LOG 收集與分析，並依照數據分析結果，確保設備效能並預測可能之資安事件。

(4) 規劃共用資料中心

統籌本府及所屬機關資訊業務的整體規劃及推動，運用整體資訊資源，以推動資訊服務雲端化、共用化與資料開放加值為主軸，經由資訊資源共用共享，減少所屬機關重複投資，創造資訊服務最大效益。

(5) 建置共用資料中心

A. 隨著近年來的環境保護意識提高及電力價格快速飛漲，綠能雲端資料中心將安全可靠之「結構化綠能機房」為首要目標，並將能源效率控制在 PUE≦1.6。能效設備，增進能源使用效率，降低資料中心整體能耗，符合政府機關建構資料中心節能減碳政策要求。

B. 確保停電時仍能提供資料中心內資訊設備持續運轉至少 30 分鐘之電力、以確保資料中心高可用性。

C. 提供實體安全、穩定的網路環境與資訊服務，並符合本府

資訊安全管理系統之規範要求。

D. 資料中心系統在異常狀況發生時，能及時切換備援系統避免服務中斷，使服務可用率達 99.95%以上。

E. 建置核心系統異地備份、備援機制。

(6) 設置虛擬主機資源池

虛擬主機的硬體將一台或多台的處理器、記憶體、磁碟，與網路資源融合，並共享出來的一個大型虛擬資源池(Virtual Resource Pool)，進而將資源池的硬體資源分享出來。同時，監測虛擬主機資源使用狀態，評估虛擬機負載，進行資源池負載平衡與虛擬機動態資源增加，以使虛擬主機維持良好運作。

2. 精進資安防護能量

(1) 導入資訊系統弱點通報機制

就既有之資訊系統弱點通報（VANS）專屬系統平台，推廣至資通安全責任等級 C 級之所屬機關（含稅務局、消防局、環保局等機關）使用，進行 VANS 資產盤點、軟體更新派送、資料介接上傳，及各項後續配套作業。

(2) 導入端點偵測及應變機制

(3) 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。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。

4. 實施範圍

（一） 臺南市政府

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

（二） 嘉義市政府

有關本計畫實施對象及實施區域，包含嘉義市政府暨所屬一、二級機關，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	擴增共用資料中心之環控系統	本市機房	建置向上集中之機房使用共用環控系統
精進資安防護能量	本府C級機關建立弱點掃描檢測系統	本府C級機關	所屬一、二級C級機關
精進資安防護能量	強化遠端連線監控及稽核	本府	本府機房

（三） 嘉義縣政府

有關本計畫實施對象及實施區域，建置及推廣2個共用性系統，並建構系統安全維運通道，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	建置及推廣共用性系統	本府、所屬機關、公所等單位	建置 EIP 入口網及表單共構系統，推廣本府、11個所屬機關及18個鄉鎮市公所使用。
	建構系統安全維運通道	本府各單位	建構系統安全維護通道暨其資安基礎建設，提供本府各單位使用。
精進資安防護能量	導入資訊系統弱點通報機制(VANS)	本縣9個C級機關	導入VANS至本縣9個資安責任等級C級機關(約1400U)。
	導入端點偵測及應變機制(EDR)	本縣3個B級機關	導入EDR至本縣3個資安責任等級B級機關(約900U)。

推動滲透測試及紅藍軍攻防演練	辦理資安檢測	本縣	辦理個人電腦及系統資安檢測。

（四） 雲林縣政府

二、 有關本計畫實施對象及實施區域，包括4間公所資訊資源向上集中、資通安全責任等級C級機關導入資訊系統弱點通報機制（VANS)、B級機關導入端點偵測及應變機制（EDR）等，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	整併線路集中網路出口	自本縣 20 個鄉鎮市公所中選擇 4 個公所辦理。	本縣所屬4個公所VPN線路與設備建置。 本府網路設備、線路擴充。包括建置WSUS伺服器、日誌（Log）蒐集系統、設置虛擬主機資源池等。
	建置共用資料中心	預計自本縣 20 個鄉鎮市公所中選擇4間公所辦理，本計畫預計分 2 年執行，逐年增加集中機關數量。	整併本縣所屬 4 間公所機關資訊機房至本府資料中心，設置虛擬主機資源池，辦理資訊系統移轉作業。預計2年計畫中，每年辦理約2個資料中心減量，及每年辦理約2至3個資訊系統移轉作業。 共用資料中心資安系統、設備、線路擴充。包括防火牆、IPS、流量管理、WSUS 伺服器、日誌(Log) 蒐集系統、集中備份系統等。 辦理 4 間公所終端電腦收容管理，採購AD 3000U授權。
精進資安防護能量	推進政府機關資訊系統弱點通報機制(VANS)	本縣所屬資通安全責任等級C級機關	推動本縣 35 個資安責任等級 C 級機關導入VANS，導入單點數量合計約4,500U。

策略面向	工作項目	實施對象	實施區域
	導入端點偵測及應變機制(EDR)	本縣所屬資通安全責任等級B級機關	推動本縣3個資安責任等級B級機關導入EDR，導入單點數量合計約3,500U。

5. 計畫期程

112年1月1日至113年12月31日。

6. 關鍵績效指標及年度目標值

（一） 臺南市政府

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導入率(導入C級機關8個/C級機關總數18個)	44%
	4	資通安全責任等級B級機關導入EDR導入率(導入B級機關3個/B級機關總數6個)	50%
	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	100%

		置提交率(導入B級機關6個/B級機關總數6個，B級機關總數6個)	
	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

（二） 嘉義市

年度	項次	關鍵績效指標	目標值
112	1	資通安全責任等級C級機關導入介接VANS導入率(導入C級機關個數/C級機關總數，C級機關總數5個，1000U)	100%

（三） 嘉義縣

年度	項次	關鍵績效指標	目標值
112	1	資通安全責任等級C級機關導入介接VANS導入率(導入C級機關個數/C級機關總數，C級機關總數9個)	100%
	2	資通安全責任等級B級機關導入EDR導入率(導入B級機關個數/B級機關總數)	100%
	3	完成資安檢測系統個數	30
113	1	資通安全責任等級B級機關導入EDR提交率(導入B級機關個數/B級機關總數)	100%
	2	完成資安檢測個人電腦台數	900

（四） 雲林縣政府

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	2

	2	資通安全責任等級C級機關導入介接VANS導入率(導入C級機關個數/C級機關總數，C級機關總數35個)	100%
	3	資通安全責任等級B級機關導入EDR導入率(導入B級機關個數/B級機關總數)	100%
113	1	完成資料中心減量個數	2
	2	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率(導入B級機關個數/B級機關總數，B級機關總數3個)	100%

7. 持續營運評估

（一） 臺南市政府

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(VANS)	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。

（二） 嘉義市政府

本計畫期程結束後，後續維運方式擬由本府各機關每年度編列預算辦理系統維運、軟體授權經費維持等，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	擴增共用資料中心之環控系統、雲端運算資源擴充	設備及系統維運	由本府每年編列預算維護：環控系統維運費用，每年預估約400仟元。
2	精進資安防護能量	導入資訊系統弱點通報機制(VANS)	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，每年預估約800仟元。
3	精進資安防護能量	遠端連線監控及稽核系統	系統授權及維護	由本府各使用機關每年編列預算維護及汰換：預估200仟元

（三） 嘉義縣政府

本計畫期程結束後，後續維運細部評估表如下：

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	1. 建置及推廣共用性系統 2. 建構系統安全維運通道	1. 共用性系統維運費用 2. 授權及維護費用	由本府各使用機關每年編列授權及維護費用約 2,700,000 元。
2	精進資安防護能量	1. 資訊系統弱點通報機制(VANS) 2. 端點偵測及應變機制(EDR)	由各機關自行編列維護預算	每年授權及維護費用約 4,810,000 元。
3	推動滲透測試及紅藍軍攻防演練	資安檢測	縮小規模辦理	由本府每 2 年編列預算持續辦理：1,500,000 元。

（四） 雲林縣

本計畫期程結束後，後續維運方式擬由本府各機關每年度編列預算辦理系統維運、網路線路租用及軟體授權經費維持等，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	整併線路集中網路出口	線路費及設備維護	由本府各使用機關每年編列預算維護：網路線路租用費用，每年約 392 仟元。網路設備維護費約原購置經費 15%，合計約 2,481 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 24 個虛擬系統，約 480 仟元。
3	精進資安防護能量	推進政府機關資訊系統弱點通報機	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 2,999 仟元。

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
		制		
4		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10,500仟元。

8. 經費明細概算

（一） 臺南市政府

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、系統軟體授、系統日誌管理。	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

	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		

（二）　嘉義市政府

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	擴增共用資料中心之環控系統	辦理向上集中之機房監控規劃與設計、電力、空調、消防等環控系統建置、雲端運算資源擴充	0	2,250,000	1	2
	2	推　廣 VANS	推動所屬 5 個資安責任等級 C 級機關導入 VANS，1000U。	3,000,000	0	5	1
	3	建　置遠　端連　線監　控及　稽核	建置本府遠端連線監控及稽核共 1 套	2,000,000	0	2(核心系統優先導入)	3
小　　計				5,000,000	2,250,000		
合　　計				7,250,000			

（三）　嘉義縣政府

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	精進資安防護能量	1. 導入資訊系統弱點通報機制(VANS) 2. 導入端點偵測及應變機制(EDR)	7,100,000	500,000	1. 推動9個C級機關導入資訊系統弱點通報機制(VANS) 2. 推動3個B級機關導入端點偵測及應變機制(EDR)	1
	2	推動滲透測試及紅藍軍攻防演練	辦理資安檢測	4,000,000	0	完成30個系統	2
小　　計				11,100,000	500,000		
合　　計				11,600,000			

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	資訊資源向上集中	1. 建置表單共構系統 2. 建置共用 EIP 入口網站 3. 建構系統安全維運通道主機代理連線、稽核、特權用戶管理機制 4. 建構系統安全維運通道雙因子認證	4,500,000	9,000,000	1. 完成表單共構系統建置 2. 完成 EIP 入口網站建置 3. 完成系統安全維運通道主機代理連線、稽核、特權用戶管理機制 4. 完成系統安全維運通道雙因	2

						子認證	
	2	精進資安防護能量	導入端點偵測及應變機制(EDR)	4,500,000	0	推動3個B級機關提交端點偵測及應變機制(EDR)偵測資料	1
	3	推動滲透測試及紅藍軍攻防演練	辦理資安檢測	5,555,556	0	完成900台個人電腦安全性檢測	3
小　　計				14,555,556	9,000,000		
合　　計				23,555,556			

（四）　雲林縣

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	整併線路集中網路出口	辦理所屬2間公所VPN線路建置。	0	518,425	完成2間公所VPN線路建置。	1
	2	建置共用資料中心	辦理2間公所資訊機房系統整併至本府資料中心。建置250個虛擬主機資源池，並辦理2個整併機關的資訊系統移轉。 基礎環境建置，包含線路向上集中整併、IPS、流量管理、	4,099,000	19,820,000	整併2間公所資訊機房至本府資料中心。	4

			線速提升、WSUS 伺服器、日誌蒐集系統、備份系統等建置。辦理 2 個整併機關終端電腦收容管理，採購 AD 1500U 授權。				
	3	推進政府機關資訊系統弱點通報機制(VANS)	導入至 35 個本府所屬 C 級機關	2,998,500	0	完成導入 VANS 至 35 個本府所屬 C 級機關。	3
	4	導入端點偵測及應變機制(EDR)	完成本縣 B 級機關導入端點偵測及應變機制（約 3500U）	0	9,135,000	完成本縣 B 級機關導入端點偵測及應變機制。	2
小　　計				7,097,500	29,473,425		
合　　計				36,570,925			

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	整併線路集中網路出口	辦理所屬 2 間公所 VPN 線路建置，以及共用系統（包含 WSUS 伺服器、日誌蒐集系統）建置。	0	722,174	完成 2 間公所 VPN 線路建置。	1

	2	建置共用資料中心	整併 2 間公所資訊機房至本府資料中心,並辦理2個整併機關的資訊系統移轉。 辦理 2 個整併機關終端電腦收容管理，採購AD 1500U授權。	0	3,737,376	整併2間公所資訊機房至本府資料中心。	3
	3	導入端點偵測及應變機制(EDR)	本府及所屬 2 個資通安全責任等級 B 級之機關導入EDR。	0	9,576,000	完成本府及所屬2個B級機關導入端點偵測及應變機制。	2
小　　計				0	14,035,550		
合　　計				14,035,550			

9. 經費補助表

（一） 臺南市政府

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

（二） 嘉義市政府

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	7,250,000	0	2,175,000	5,075,000

年				

（三） 嘉義縣政府

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	11,600,000	0	1,160,000	10,440,000
113 年	23,555,556	0	2,355,556	21,200,000

（四） 雲林縣政府

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	36,570,925	0	7,314,185	29,256,740
113 年	14,035,550	0	2,807,110	11,228,440

10. 預定進度

（一） 臺南市政府

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)

（二） 嘉義市政府

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
112/9	41%	3,000,000	完成導入所屬 5 個資安責任等級 C 級機關導入 VANS，1000U。

112/12	100%	7,250,000	完成擴增共用資料中心之環控系統及雲端運算資源擴充。(同步完成建置遠端連線監控及稽核)

(三) 嘉義縣政府

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
112/9	61%	7,100,000	1.推動 9 個 C 級機關導入資訊系統弱點通報機制(VANS) 2.推動 3 個 B 級機關導入端點偵測及應變機制(EDR)
112/12	100%	11,600,000	完成 30 個系統安全性檢測

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
113/8	38%	9,000,000	1.完成表單共構系統建置 2.完成 EIP 入口網站建置
113/12	100%	23,555,556	1.完成系統安全維運通道主機代理連線、稽核、特權用戶管理機制 2.完成系統安全維運通道雙因子認證 3.推動 3 個 B 級機關提交端點偵測及應變機制(EDR)偵測資料 4.完成 900 台個人電腦安全性檢測

(四) 雲林縣

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
112/3	8.2%	2,998,500	完成導入 VANS 至 35 個本府所屬 C 級機關
112/6	33.2%	12,133,500	完成本府及所屬 B 級機關導入端點偵測及應變機制
112/12	100%	36,570,925	1.整併 2 間公所資訊機房之共用系統至本府資料中心 2.完成 2 間公所網路整併、VPN 線路建置

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
113/3	68.2%	9,576,000	完成本府所屬 2 個 B 級機關導入端點偵測及應變機制
113/12	100%	14,035,550	1.2 間公所資訊機房系統整併至本府資料中心 2.完成 2 間公所 VPN 線路建置

11. 預期效益

（一） 臺南市政府

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。

（二） 嘉義市政府

項次	工作項目	預期效益

1	擴增共用資料中心之環控系統	1. 增進共用資料中心實體安全，即時掌控機房人員進出情形，並能在第一時間回報異常。 2. 針對機房內物聯網偵測器或監控系統進行檢測，檢討並提供完善資安防護。 3. 雲端運算資源擴充，精進系統使用效能。
2	推廣 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。

（三） 嘉義縣政府

項次	工作項目	預期效益
1	建置及推廣共用性系統	1. 建置 EIP 入口網站及表單共構系統，推廣本府、11 個所屬機關及 18 個鄉鎮市公所使用。 2. 完成本縣共構應用系統服務，集中有限資源，統籌控管與運用，提升資源運用效率及縮減資安防護缺口。
2	建構系統安全維運通道	建構主機代理連線、稽核及特權用戶管理機制、雙因子驗證系統暨其資安基礎建設，提供系統安全維運通道，防堵或封鎖駭客入侵管道，兼顧系統維運需求與資安問題，提升整體資安防護能力。
3	導入資訊系統弱點通報機制(VANS)	1. 落實資通安全管理法應辦事項。 2. 強化資訊資產弱點管理及控管。
4	導入端點偵測及應變機制(EDR)	建置及佈署端點威脅防禦系統，補強其他資安防護系統之不足，快速反應資安問題，精進資安防護能量。
5	辦理資安檢測	委請資訊安全檢測專家辦理資安檢測，改善個人電腦及系統的弱點，提升資訊安全。

（四） 雲林縣政府

項次	工作項目	預期效益
1	整併線路集中網路出口	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. 整併重複之資訊系統或服務，減少所屬機關重複投資，創造資訊服務最大效益。 2. 增進能源使用效率。 3. 資訊資源統籌管理，降低基層機關之資安風險。
3	推進政府機關資訊系統弱點通報機制（VANS）	1. 落實資通安全責任等級 C 級以上之公務機關應辦事項。 2. 有效管理使用者端軟體，避免使用者任意安裝。 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	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。

12. 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	06-2991111#8060	ite141@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
嘉義市政府智慧科技處資通建設科	林萬豐	05-2254321#764	wflin@ems.chiayi.gov.tw
嘉義縣政府綜合規劃處資訊管理科	侯淨涔	05-3620123-8243	jingcen@mail.cyhg.gov.tw
雲林縣政府計畫處	莊齊珉	05-5522994	ylhg02169@mail.yunlin.gov.tw

資管科			
雲林縣政府計畫處 資管科	洪詠倫	05-5522997	ylhg02171@mail.yunlin.gov.tw
雲林縣政府計畫處 資管科	林欣生	05-5522990	ylhg02118@mail.yunlin.gov.tw

附件6

政府基層機關資安主動防禦之分項計畫

高雄市政府(含屏東縣、澎湖縣、臺東縣政府)

計畫全程：112年1月至113年12月

112－113 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 年至 113 年度前瞻基礎建設「政府基層機關資安主動防禦計畫」，推動資訊資源向上集中，持續精進第一階段前瞻計畫區域聯防之資安防護能量，並推動滲透測試及紅藍軍攻防演練及研提創新之服務。

現今政府部門行政環境資訊化高度發展，資源向上集中已成為趨勢。建立自己的私有雲（Private Cloud）加強虛擬化平台管理以及各虛擬機（Guest VM）之間網路安全儼然是當下課題。

在行政院的協助下，於 107 年至 109 年前瞻計畫第一階段中已完成結合屏東縣、臺東縣及澎湖縣等縣市政府聯合建構資安區域聯防體系，有效建立地方聯合資訊安全防護網。

於整體區域的資安防護工作推動上，已陸續協助基層機關進行老舊個人電腦設備汰換、網路架構集中整併、納入 SOC（Security Operation Center）7*24 監控機制管理及導入政府組態基準（GCB）、建立端點監控防護、資通安全責任等級 B 級機關導入資訊系統弱點通報機制（VANS）等資安防護監控機制，有效強化基層機關資安防護縱深能量，達成資安政策一致性的要求，並協助基層機關瞭解與發現駭客企圖與偵測機關資安事故及缺失，即時通報應變、鑑識分析、追蹤處理。

為推動打造堅韌安全之智慧國家賡續推動政府資訊資源集中共享的政策指導方針，以及考量本區域縣市政府資通訊系統與安全防護現況所需，擬定「高雄市、屏東縣、澎湖縣、臺東縣政府 112－113 年前瞻基礎建設－政府基層機關資安主動防禦計畫」。

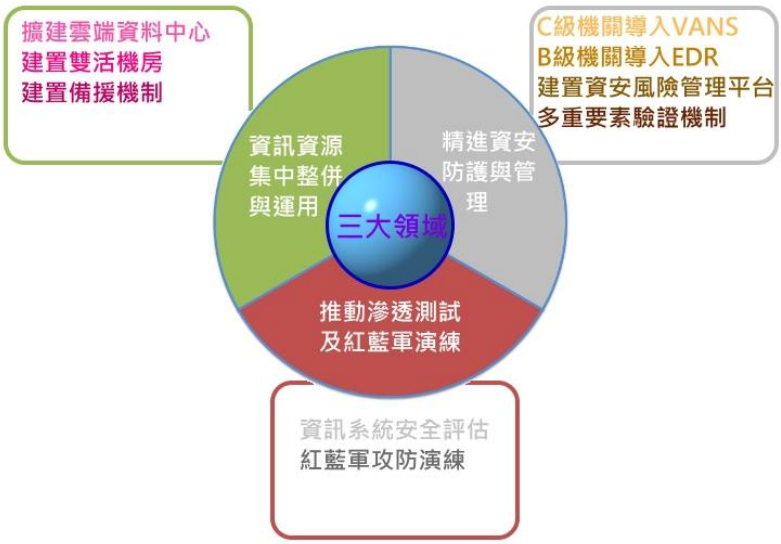
二、 計畫目標

（一） 高雄市政府

1. 資訊資源向上集中：於本計畫中將建置完善備援機制並擴充雲端資料中心平台方案，供轄下機關使用共用資源，預計減少 2 個小型機房，達到機房減量之目標。

2. 精進資安防護能量：配合推動政府機關資訊系統弱點通報機制，將持續將C級機關納入通報機制，B級機關導入端點偵測及應變機制(EDR)，確保所有基層機關都具備一定強度的防禦能力，不因為某一機關防禦強度不足，而影響整體防禦能量，以期健全整體資安體質，強化資安基礎建設使端點資安等級更加提升。
3. 推動紅藍軍攻防演練：為強化本府資安防護能量，本計畫規劃以紅藍軍資安攻防演練方式，提出3種模擬情境，由駭客(紅軍)進行複合性攻擊，本府(藍軍)進行資安偵測監控、緊急應變、採證鑑識以及弱點漏洞修補等相關措施。

整體計畫目標將包含三大領域：資訊資源向上集中、精進資安防護能量、推動紅藍軍攻防演練。其中以向上、精進、攻防等三個元素完美結合，完善整體區域資安防護作為。



（二） 屏東縣政府

1. 精進資安防護能量
   （1） 完成符合資通安全責任等級C級以上之機關均導入資訊系統弱點通報機制(VANS)。
   （2） 完成符合資通安全責任等級B級之機關均導入端點偵測及應變機制(EDR)。

（三） 澎湖縣政府

1. 擴增本府資料中心運作能量，提供有效且充足的餘裕運作空間及效能，推動機房資源整併共用，持續減少所屬機關小型機房數至少 2 個。
2. 共用性系統向上集中維運管理，降低整體維運管理成本，有效提升系統防護等級。
3. 完成符合資通安全責任等級 C 級以上之機關均導入資訊系統弱點通報機制(VANS)。
4. 完成符合資通安全責任等級 B 級之機關均導入端點偵測及應變機制(EDR)；並依指定之方式提交端點偵測及應變機制(EDR)偵測資料。
5. 精進本府與線路整併基層機關端整體網路安全防護機制，厚實整體資安防護縱深能量，強化資安區域聯防體系機制。
6. 確保所有基層機關都具備一定強度的防禦能力，不因為某一機關防禦強度不足，而影響整體防禦能量，以期健全整體資安體質，強化資安基礎建設。
7. 完備異地備份儲存機制，確保備份資料完整性及有效性。

（四） 臺東縣政府

1. 本計畫以「精進本府及所屬之資安防護能量(導入 VANS、EDR)」為目標。
2. 輔以資訊系統弱點通報機制(VANS)之 MBSA 工具提升微軟系列產品安全性，並提高整體資安防護量能。

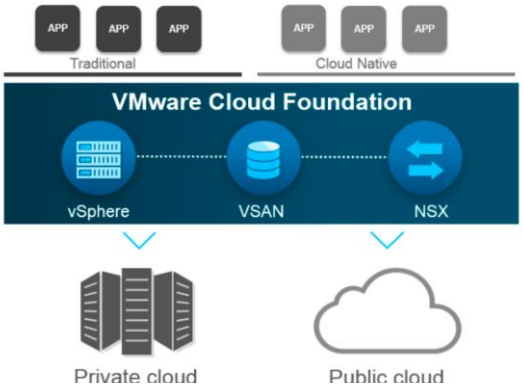
三、 計畫內容與實施策略

（一） 高雄市政府

1. 資訊資源向上集中

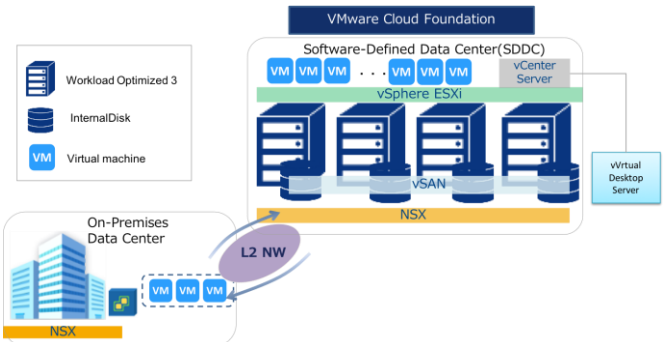
本計劃將以本府雲端資料中心為基礎，擴建現有資訊資源平台增加收容小型機房範圍，且建置一套異地備援系統平台，提供整併至本府雲端資料中心之系統，能有完善的備援機制，達成向上集中之目標，做為資訊資源向上集中之典範。

(1) 擴充本府資料中心平台系統



「110 年強化政府基層機關資安防護計畫」，本府已將工務局、違建大隊、新工處、觀光局、文化局、毒防局、原民會、捷運局、環保局、社會局等小型機房，統一向上集中至本府共用機房，並共享使用虛擬化資源，已達到資訊資源向上集中之目標；為更完善本府向上集中之方向，本計劃將擴充現有之雲端資料中心平台系統，提供更多共用資源，且預計減少 2 個小型機房，達到機房減量之目標；並提供自動化佈署虛擬機之機制，供移轉機關運用與管理；以減少實體機之使用，降低機房環境之負載，使資訊資源更有效的運用。本府規劃透過已建置之虛擬化系統技術，將實體機之系統移轉至集中式共享雲端基礎平台上；透過平台自動化管理與監控機制，使系統運作狀況能隨時掌握，且集中式的管理使資安等級能落實資安規範。

現今環境已經慢慢轉變為虛擬化部署的 IT 時代，可以達到集中化快速部署及管理已理想目標。這時就必須在現行的架構內，加入可強化監視、診斷以及控制的管理工具，增加虛擬化基礎架構的可見度，讓任何與整體運作上有關的效能、容量、可靠度、可用性等問題，都能夠藉由大量數據的收集與分析，進而達到事前防範或是即時解決的效益。



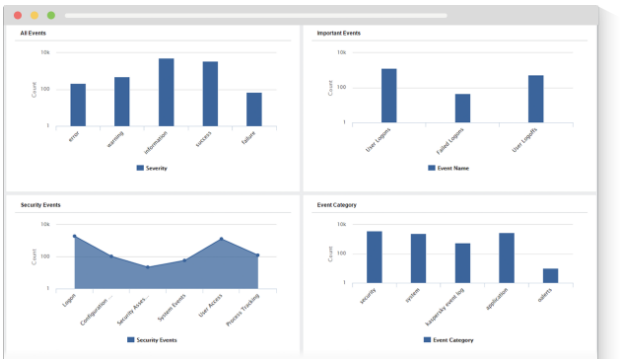
(2) 建置資料中心備份平台及備援機制

本府雲端資料中心除已建置高可用性之系統平台外，亦需佈署完整可保護整個混合式雲端基礎架構，包括實體系統、虛擬機管理程式和 VM、雲端應用程式等之備份還原系統，透過集中管理與統一介面，來管理各種形式的資料保護，將資料備份至儲存空間，及易於復原任何資料，以最大程度減少因災難發生而產生停機時間。

因此本府規劃擴充原雲端資料中心備份還原系統之備份範圍，完整保護整個市府雲端資料中心之系統與資料，提升市府服務水平。

另本府資料中心已具備備份機制，因此為提供更高可用性之雲端平台，規劃於本府鳳山行政中心建置一備援系統，除了於異地備份的方式來確保資料及系統之安全外，透過建置 Globe Server Loading Balance（GSLB）設備於四維行政中心、鳳山行政中心，達到 DNS 服務異地備援服務之成效，使四維行政中心服務中斷時，由異地備援之系統接手營運，使重要系統服務不為中斷。

一個完整的資料中心，除建置虛擬化平台、雲端服務、資安防護、完整備份備援及確保網路服務不中斷外，針對平台上之 Guest VM 系統，亦需確保 syslog 及 WebLog（如 IIS、Apache 等）之同步保存安全，避免駭客入侵時，同時將其軌跡刪除，造成日後資安事件鑑識之困難，難以彌補已遭入侵之漏洞；本府規劃建置 Log 紀錄收集分析平台，同步將其 Log 做妥善備份，保留完整入侵軌跡，且藉由平台分析與報表功能，來進行紀錄管理、安全紀錄檔管理、事件紀錄檔監視、應用程式紀錄監視、網路裝置稽核等功能。



(3) 備援資料中心網路環境建置

資訊資源集中化，備援提供服務更是不可忽略的，完備的備援資安防護不僅能提供更好的服務，也更能有效的使用設備資源。

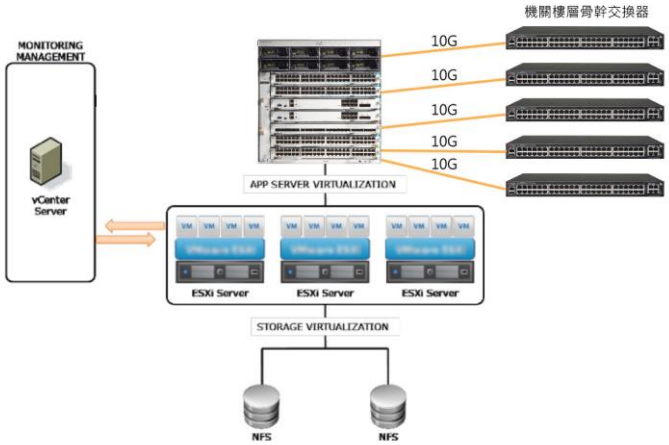
本府規劃於鳳山行政中心機房改以備援機房提供本府雲

端資料中心之備援機制，並於該場域建置一路對外線路，做為備援對外服務之線路所使用；並以 GSLB 設備，形成雙活機房環境。

（4）擴充本府資料中心網路環境

隨著網路應用及需求日益倍增，且因應雲端資料中心的建置，資料的儲存也將隨之大量成長，伴隨著網路頻寬的需求便增高，現行機關至機房之間的 1G 傳輸頻寬便不敷使用，短時間多人存取、大量資料讀寫、雲端服務等便需藉由內部頻寬之提升，來解決頻寬壅塞之問題。

隨著原舊有 11 個小型機房整併至本府雲端資料中心，且機房骨幹核心交換器已提升至 10G 介面，並以 HA 方式提供服務，部分機關至機房之骨幹已提升至 10G 網路頻寬，為使本府頻寬串接皆為 10G，本計畫將剩於尚未提升頻寬之機關，全面汰換建置成 10G 樓層骨幹交換器共 28 部，降低頻寬壅塞現象及加速雲端平台之傳輸速率，現有舊型之交換器則做為備援之使用。



2. 精進資安防護能量

（1）本府 C 級機關導入政府機關資安弱點通報機制（VANS）

為推廣政府機關資安弱點通報機制（VANS），本府已於 111 年部署 B 級機關 VANS 系統，並介接技術服務中心的 VANS 且回報相關訊息，本規劃將於 112 年將其機制推廣至本府 C 級機關，並定期將保有的軟體項目清單轉換為 CPE 格式自動傳至 VANS，與 NVD 弱點資料庫比對最新的弱點資訊

後，將比對完成的結果再介接回到本府軟體資產管理平台，產出各主機需要更新的軟體清單，再經由軟體派送功能，針對平台上已知各主機應更新的軟體，以軟體派送功能，取代由人工逐台安裝主機的軟體更新。

預計 112 年導入 11,206 台機關內電腦及資訊系統主機皆應納入本府軟體資產管理平台，由機關管理者妥善管理。計畫時程及範圍：

年度	導入機關數量（C 級）	端點數量
112 年	44	11,206

（2）端點偵測及應變機制（EDR）偵測服務

依據「資通安全責任等級分級辦法」規定，資通安全責任等級 B 級之公務機關需建置端點偵測及應變機制導入；本府於 107 年至 109 年前瞻計畫中，針對重要伺服主機與端點已導入 APT 進階持續性威脅系統服務，為配合「資通安全責任等級分級辦法」規定，規畫本府 B 級機關全面部署 EDR 服務，針對所有可疑活動或警報，在專業技術團隊的分析與判斷中，防範未知的攻擊手法，及早發現潛在資安威脅，主動阻斷駭客組織的惡意攻擊，降低資安誤判的預期。透過即時事件處理，除降低損失外，也能持續分析攻擊者的入侵過程，持續強化整個環境防護。

預計 112 年導入 11 個 B 級機關 4480 台機關內電腦及資訊系統主機皆應納入端點偵測及應變機制（EDR）偵測服務，113 完成年 11 個 B 級機關 4480 台機關內電腦及資訊系統主機提交 EDR 至主管機關指定位置功能服務。

計畫時程及範圍：

導入機關數（B級）	年度	
	112年	113年
11個機關導入數量	4480	4480
執行範圍	導入EDR服務	完成EDR指定位置功能

(3) 建置資安風險管理防禦平台

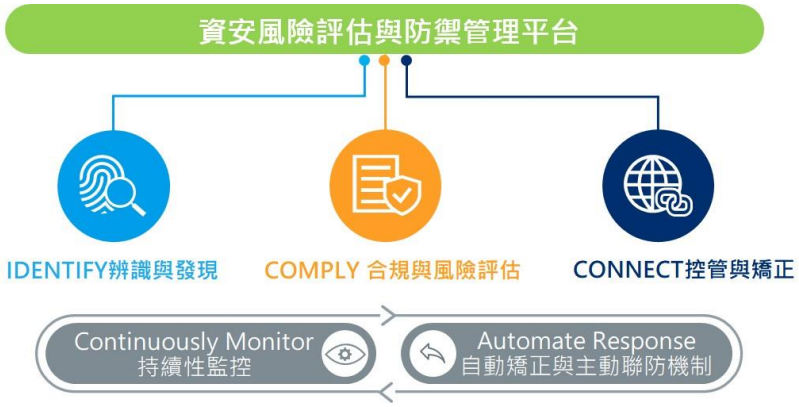
本府導入之端點偵測回應（EDR）系統可針對安裝EDR軟體的端點裝置進行資安事件分析，但對於未安裝EDR或有意、無意不安裝EDR之終端設備則無法管制，使得EDR系統導入時間越久，EDR端點數越來越少，因此造成資安的死角。

因此，本府將規劃資安風險評估與防禦管理平台（簡稱為資安管控平台），針對終端裝置進行主動偵測與設備類型識別，當檢測到未安裝EDR軟體或不符本府資安要求（例如：未安裝GCB、VANS、防毒軟體...等）、具有雙網卡等具有風險的裝置時，可禁止其存取網路，隔離不符規定的設備，降低發生資案事件的機率。

除此之外，當內部電腦被入侵嘗試對外連線時，本府的資安設備可阻擋其連線，使其無法將資料外傳，但已被入侵的電腦還是可透過府內網路，去感染府內的其他電腦。而資安管控平台可與本府的資安設備進行聯防，資安設備可將log轉送至資安管控平台，資安管控平台可針對有問題的電腦透過代理程式進行網路隔離，而對於未安裝代理程式的電腦，也可整合本府既有的網路交換器進行聯防機制，將其隔離於某一區域中，可大幅縮小被感染電腦數量，將損害降到最低。

預計113年導入2300台機關內電腦及資訊系統主機皆

納入資安管控平台系統。



計畫目標：

計畫時程及範圍：

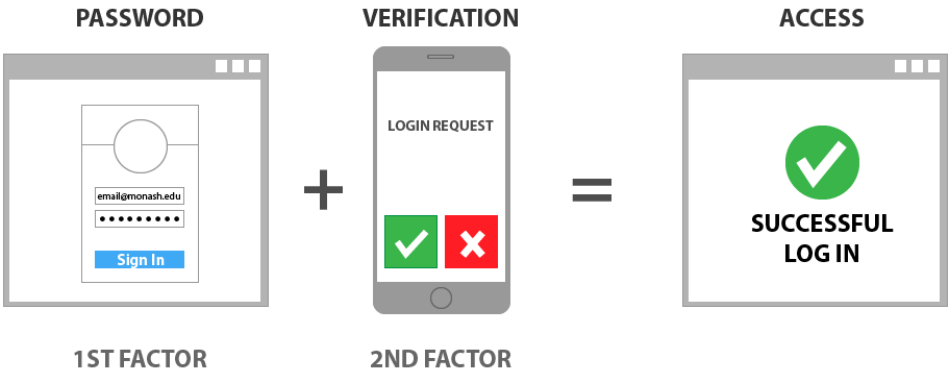
導入機關數（B 級）	年度
	113 年
11 個機關導入數量	2300

(4) 多重要素驗證(MFA)機制

一個完善的資安防禦架構會有許多的資安設備或系統，如果僅使用密碼來驗證使用者，將會有不安全的媒介可能遭到攻擊。尤其是資訊資源向上集中化的架構上，密碼的安全就更為重要了。如果密碼安全等級很弱，或已在別處公開，攻擊者便可以輕易的透過合法方式來取得存取權。 因此，有鑑於單一帳號認證機制不夠周全，當帳號遺失後可能造成府內系統被有心人士入侵，為使本府已向上集中之共用資源具備高安全性之環境，因此本府規劃導入多重要素驗證系統。

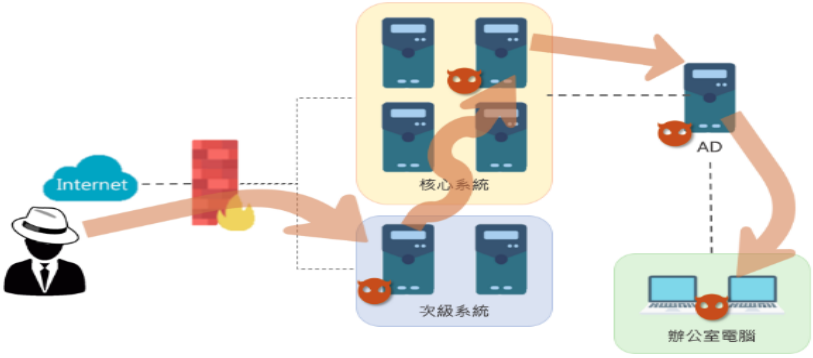
當管理人員登入系統或網路設備時，除了輸入帳號與密碼之外，還需透過手機 APP、email 或簡訊等方式獲得另一

組多重要素驗證的密碼，來進行第二次認證以確認登入者的身分，避免帳號被冒用的狀況產生。



3. 推動紅藍軍攻防演練

為補足傳統滲透測試容易忽略之邊界防禦，以及基於人為疏失之佈署盲點，本府規劃辦理紅藍軍攻防演練，由社群專家、白帽駭客或專業資安團隊擔任攻擊方(紅隊)，利用公開資訊、社交網路、暗網等搜集目標情資、結合專業知識、攻防技術及駭客工具資料庫，對於所約定之攻擊目標與組織，採取無所不用其極的方法進行入侵演練，同時驗證防守方(藍隊)的偵測監控、緊急應變、採證鑑識以及弱點漏洞修補能力，達到資安攻防演練效果。



（二） 屏東縣政府

1. 精進資安防護能量

本府配合資通安全管理法之施行，已執行資訊安全管理系統之導入及通過公正第三方之驗證、內部資通安全稽核、業務持續運作演練、資安治理成熟度評估、限制使用危害國家資通安全產品、網站安全弱點檢測、系統滲透測試、資通安全健診、資通安全威脅偵測管理機制、政府組態基準、資通安全防護、資通安全教育訓練等各項應辦事項，取得資通安全專業證照及職能訓練證書，並加入由高雄市政府建置之資安區域聯防平台(K-ISAC)聯防成員及完成自動化派送防護規則。

本計畫規劃導入資訊系統弱點通報機制(VANS)及端點偵測及應變機制(EDR)。VANS 藉由軟體工具清點使用者電腦安裝之軟體，統一彙報。若接獲軟體具有漏洞或資安疑慮之更新，將可進一步了解使用者電腦安裝軟體需進行漏洞修補或更新之概況。EDR 將於使用者電腦識別攻擊者行為，進行防禦威脅與回應警示。

本府、本府所屬警察局、財稅局(資安責任等級皆為 B 級)已於 110 年導入資訊系統弱點通報機制(VANS)，本計畫規劃 112 年起，於 B 級機關導入端點偵測及應變機制(EDR)。藉由自動化識別攻擊者行為、分析個人電腦異常行為，快速進行防禦威脅與回應警示。

此外，本計畫亦規劃於 112 年起，本府所屬環境保護局、衛生局、消防局(資安責任等級皆為 C 級)導入 VANS。定期清查軟體資訊資產，經由 CPE 清單比對，管控軟體潛在之風險與弱點，評估修補規劃。

資訊系統弱點通報機制(VANS)可將單位內安裝之軟體資產，自動化完成 CPE 報表，並透過技服中心提供之軟體弱點資訊，取得弱點修補評估報告。輔以軟體部署工具進行修補軟體更新，降低零時差惡意探索之資安風險，提高資安防禦能力。

端點偵測及應變機制(EDR)可識別攻擊者行為，經由部署

檢測和回應工具，透過自動化和機器學習，自動執行調查以加快回應速度，學習與分析終端設備活動、發現隱匿的威脅。

端點偵測及應變機制(EDR)：

項次	導入機關	數量
1	屏東縣政府(B級)	955
2	屏東縣政府警察局(B級)	430
3	屏東縣政府財稅局(B級)	260

資訊系統弱點通報機制(VANS)：

項次	導入機關	數量
1	屏東縣政府環境保護局(C級)	50
2	屏東縣政府衛生局(C級)	200
3	屏東縣政府消防局(C級)	100

（三） 澎湖縣政府

1. 擴增本府資料中心運作能量，推動機房資源整併共用

(1) 擴增本府資料中心整體運作能量，維持有效且充足的餘裕運作空間及效能，提供機房整併所需之主機運作資源；避免機房資源整併共用後，因資源或空間不足，造成無法正常切換轉移或完成快照及備份，造成服務停擺。

(2) 本府目前已經整併本府13個府內單位、2個所屬一級機關、1個所屬二級機關及6個鄉市公所機房向上集中工作，將至少再整併2個C級機關（環境保護局、衛生局或地政事務所）小型機房設備。

(3) 降低新設實體主機或減少現有實體主機數量。

(4) 改善資料中心基礎設施運作環境，維持資料中心整體安全性、可靠性及高可用性。

(5) 運用共同供應契約採購或依據政府採購法相關規定以公開招標方式辦理。

2. 精進本府與基層機關整體網路安全防護機制，強化線路整併機

關端網路連線監控環境與防禦能量

(1) 推動符合資通安全責任等級C級之機關均導入資訊系統弱點通報機制(VANS)。

(2) 推動符合資通安全責任等級B級之機關均導入端點偵測及應變機制(EDR)；並依指定之方式提交端點偵測及應變機制(EDR)偵測資料。

導入機關與數量：

項次	導入機關	數量
1	澎湖縣政府(B級)	750
2	澎湖縣政府警察局(B級)	675
3	澎湖縣政府稅務局(B級)	60
4	澎湖縣政府消防局(C級)	60
5	澎湖縣政府衛生局(C級)	110
6	澎湖縣政府環境保護局(C級)	100
7	澎湖縣政府文化局(C級)	80
8	澎湖縣澎湖地政事務所(C級)	55
9	澎湖縣馬公市第一衛生所(C級)	30
10	澎湖縣馬公市第二衛生所(C級)	20
11	澎湖縣湖西鄉衛生所(C級)	30
12	澎湖縣白沙鄉衛生所(C級)	25
13	澎湖縣西嶼鄉衛生所(C級)	20
14	澎湖縣望安鄉衛生所(C級)	20
15	澎湖縣七美鄉衛生所(C級)	15
合計		2,050

(3) 汰換老舊且原廠不再提供軟體技術支援更新之資安防護與網路設備。

(4) 因應本縣基層機關（單位）出口端線路集中至縣府統一出口資安防護所需，強化本府與線路整併基層機關網路行為監

控、分析與防禦能力。

(5) 建立日誌收集管理機制：針對不同設備的事件資訊進行標準化、格式化，予以處理分析，便於監控與針對可疑事件採取相關行動。

(6) 運用資安專業技術人力，協助本府與基層機關辦理相關資安防禦、監測與分析工作，提升資安防護能量。

(7) 運用共同供應契約採購或依據政府採購法相關規定以公開招標方式辦理。

3. 完備異地備份儲存機制

(1) 因應資訊系統向上集中資料備份儲存安全性需求，維持自動化備份機制有效的備份週期與空間，確保備份資料安全有效。

(2) 運用共同供應契約採購或依據政府採購法相關規定以公開招標方式辦理。

(四) 臺東縣政府

1. 精進資安防護能量

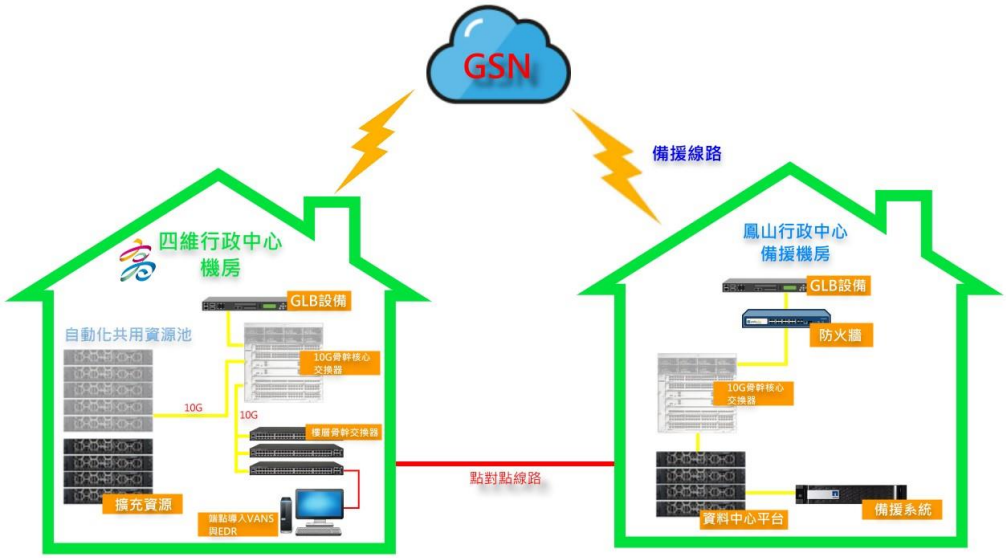
(1) 推動本縣資安等級C級機關(衛生局、消防局)導入資訊系統弱點通報機制（含通訊費）(VANS)。

(2) 持續推動110年已導入資訊系統弱點通報機制(VANS)單位之維運作業。

(3) 運用資訊系統弱點通報機制(VANS)之第三方工具MBSA功能，以強化安全性更新之落實。

(4) 推動2個B級機關及2個C級機關導入端點偵測及應變機制(EDR)，並持續維持109年建置之16個公所、4個地政事務所、1個戶政事務所端點偵測及應變機制（含通訊費）(EDR)，並新增主動阻斷機制。

四、 實施範圍



高雄市政府資料中心建構藍圖示意圖

（一） 雲端資料中心平台建置區域範圍包含四維行政中心機房為主機房，鳳山行政中心機房為資料中心備援機房，實施對象為區域內各縣市政府及轄下機關。

（二） 本區域各縣市政府佈署政府機關資安弱點通報機制（VNAS）實施對象為所有 C 級機關端點。

（三） 本區域各縣市政府佈署端點偵測及應變機制（EDR）實施對象為所有 B 級機關端點。

（四） 屏東縣政府計畫實施對象為本府資訊機房、網路，資訊系統伺服器及使用者電腦資安服務，實施區域包含本府及所屬一級機關。

（五） 澎湖縣政府計畫實施對象為縣府及所屬基層機關與各鄉市公所。

（六） 臺東縣政府端點偵測及應變機制(EDR) 實施對象為縣府及 16 個公所、4 個地政事務所、1 個戶政事務所、3 個所屬一級、府外社會處、府外文化處共計 27 個單位。

（七） 高雄市辦理「推動紅藍軍攻防演練」
以本府作為實施範圍，並且提供 3 種模擬情境，執行紅藍軍資安攻防演練。

五、 計畫期程

本計畫自 112 年 1 月起至 113 年止，共計 2 年，並依照行政院補助計劃核可費用實施。

六、 關鍵績效指標及年度目標值

區域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	1
	2	C 級機關導入政府機關資安弱點通報機制（VANS）導入率(導入 C 級機關個數/C 級機關總數，高雄市 C 級機關總數 44 個、屏東縣 3 個、澎湖縣 12 個、臺東縣 2 個)	100%
	3	C 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	<30%
	4	資通安全責任等級 B 級機關導入 EDR 導入率(導入 B 級機關個數/B 級機關總數，高雄市 B 級機關總數 11 個、屏東縣 3 個、澎湖縣 3 個、臺東縣 2 個)	100%
	5	紅藍軍資安攻防演練之模擬情境個數	1
113	1	完成資料中心減量個數	3
	2	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率(導入 B 級機關個數/B 級機關總數，高雄市 B 級機關總數 11 個、屏東縣 3 個、澎湖縣 3 個、臺東縣 2 個)	100%
	3	紅藍軍資安攻防演練之模擬情境個數	2

各縣市詳細關鍵績效指標及年度目標值

（一） 高雄市政府

年度	項次	關鍵績效指標	目標值
112	1	C 級機關導入政府機關資安弱點通報機制（VANS）導入率(導入 C 級機關個數/C 級機關總數，C 級機關總數 44 個)	100%
	2	資通安全責任等級 B 級機關導入 EDR 導入率(導入 B 級機關個數/B 級機關總數，B 級機關總數 11 個)	100%
	3	紅藍軍資安攻防演練之模擬情境個數	1
113	1	完成資料中心減量個數	2

	2	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率(導入B級機關個數/B級機關總數，B級機關總數11個)	100%
	3	紅藍軍資安攻防演練之模擬情境個數	2

（二） 屏東縣政府

年度	項次	關鍵績效指標	目標值
112	1	資通安全責任等級C級機關導入介接VANS導入率(導入C級機關個數/C級機關總數，C級機關總數3個)	100%
	2	資通安全責任等級B級機關導入EDR導入率(導入B級機關個數/B級機關總數，B級機關總數3個)	100%
113	1	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率(導入B級機關個數/B級機關總數，B級機關總數3個)	100%

（三） 澎湖縣政府

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	1
	2	資通安全責任等級C級機關導入介接VANS導入率(導入C級機關個數/C級機關總數，C級機關總數12個)	100%
	3	資通安全責任等級B級機關導入EDR導入率(導入B級機關個數/B級機關總數，B級機關總數3個)	100%
	4	擴充本府資料中心運作能量(累計)	15%
	5	資通訊系統實體設備減量率(累計)	80%
	6	提高硬體設備運作資源使用率(累計)	35%
	7	完備異地備份儲存機制(累計)	35%
113	1	完成資料中心減量個數	1
	2	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率(導入B級機關個數/B級機關總數，B級機關總數3個)	100%
	3	擴充本府資料中心運作能量(累計)	30%
	4	資通訊系統實體設備減量率(累計)	90%
	5	提高硬體設備運作資源使用率(累計)	45%

	6	完備異地備份儲存機制(累計)	100%
	7	建立日誌收集管理機制(累計)	100%

（四） 臺東縣政府

年度	項次	關鍵績效指標	目標值
112	1	資通安全責任等級C級機關導入介接VANS導入率(導入C級機關個數/C級機關總數，C級機關總數2個)	100%
	2	資通安全責任等級B級機關導入EDR導入率(導入B級機關個數/B級機關總數，B級機關總數2個、、C級機關總數2個)	100%
113	1	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率(導入B級機關個數/B級機關總數，B級機關總數2個、C級機關總數2個)	100%

七、 持續營運評估

（一） 共用雲端資料中心之軟硬體設施，於計畫期程結束後，依本府已訂定之「高雄市政府資訊中心虛擬化主機平台管理要點」辦理（https://outlaw.kcg.gov.tw/LawContent.aspx?id=GL001400），以使用者付費之原則，將請各機關自籌經費，共同維持軟、硬體之維運。

（二） 資訊硬體設備保固期由廠商提供維護及相關服務。

（三） VANS、EDR及部分服務系統將由本府持續編列維護預算，以維持系統正常營運。

八、 經費明細概算

（一） 高雄市政府

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	建置資料中心骨幹交換器40G模組	0	1,100,000	1.完成異地備援機制，形成雙活機房。 2.資料中心對外傳輸頻寬提升	1
			建置資料中心骨幹交換器10G模組	0	1,200,000		
			建置虛擬化系統備援	3,100,000	0		

			系統			至40G。	
			建置異地端備援廣域式負載平衡系統	0	3,358,572	3.提供50TB異地備援儲存空間。	
			建置異地端虛擬化系統備援伺服主機	0	3,000,000	4.提供異地備援機房對外服務線路。	
			建置異地端虛擬化系統備援軟體	3,279,000	0		
			建置異地端備援虛擬化管理軟體	800,000	0		
			建置異地端虛擬化作業系統授權	2,500,000	0		
			建置異地端虛擬化系統備援儲存設備	0	5,000,000		
			建置異地端對外服務線路	3,239,571	0		
			小計	12,918,571	13,658,572		
	2	精進資安防護能量	建置C級政府機關資安弱點通報機制(VANS)	0	16,000,000	1.完成44個C級機關導入VANS系統。	2
			建置B級機關導入端點偵測及應變機制(EDR)	21,000,000	0	2.完成11個B級機關導入端點偵測及應變機制(EDR)達100%。 3.完成11個B級機關50%重要端點導入資安風險管理系統。	
			小計	21,000,000	16,000,000		

	3	推動紅藍軍攻防演練	1. 由社群專家、白帽駭客或專業資安團隊擔任攻擊方(紅隊)，利用公開資訊、社交網路、暗網等搜集目標情資、結合專業知識、攻防技術及駭客工具資料庫，對於所約定之攻擊目標與組織，採取無所不用其極的方法進行入侵演練。 2. 驗證本府(藍隊)的偵測監控、緊急應變、採證鑑識以及弱點漏洞修補能力。	7,000,000	0	1. 執行 1 個模擬情境之紅藍軍資安攻防演練。 2. 預計 3 個不同社群專家、白帽駭客或專業資安團隊擔任攻擊方(紅隊)。 3. 初步檢測本府至少 1000 個 IP。 4. 每 1 個攻擊方須提交 1 份初測報告及複測報告。 5. 演練作業結束後，須提交 1 份完整「攻防演練技術服務成果報告書」，內容至少應包含測試過程執行之各項細節說明、初測報告、複測報告以及協助本府完成弱點漏洞修補說明。	3
			小計	7,000,000	0		
小　　計				40,918,571	29,658,572		
合　　計					70,577,143		

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	資訊資源向上集中	擴充虛擬化平台軟體	0	7,020,000	1.減少2個小型機房。 2.增加75台需擬機運作能量。 3.擴增50TB儲存空間，增加收容量。 4.提供100TB Log資料儲存空間。 5.完全28部樓層交換器更新。	1
			擴充雲端平台作業系統授權	0	2,047,000		
			擴充資料中心伺服主機	0	3,150,000		
			擴充虛擬化備份軟體	0	2,664,428		
			建置Log備份系統	0	1,638,000		
			建置Log備份儲存設備	0	819,000		
			建置樓層骨幹交換器	0	5,733,000		
			小計	0	23,071,428		
	2	精進資安防護能量	建置B級機關導入端點偵測及應變機制(EDR)	30,000,000	0	1.完成11個B級機關提交EDR至主管機關指定位置提交率達100%。 2.完成11個B級機關均導入資安風險管理系統。 3.完成資安設備多重要素驗證系統。	2
			建置資安風險管理防禦平台	0	9,500,000		
			建置多重要素驗證(MFA)機制	3,884,286	0		
			小計	33,884,286	9,500,000		
	3	推動紅藍軍攻防演練	1.由社群專家、白帽駭客或專業資安團隊擔任攻擊方(紅隊)，利用公開資訊、社交網路、暗網等搜集目標情資、結合專業知識、攻防技術及駭客工具資料庫，對於所約定之攻擊目標與組織，採取無所不用其極的方法進行入侵演練。 2.驗證本府(藍隊)的偵測監控、緊急應	15,000,000		1.執行2個模擬情境之紅藍軍資安攻防演練。 2.預計6個不同社群專家、白帽駭客或專業資安團隊擔任攻擊方(紅隊)。 3.初步檢測本府至少1000個IP。 4.每1個攻擊方須提交1份初	3

			變、採證鑑識以及弱點漏洞修補能力。			測報告及複測報告。 5.演練作業結束後，須提交1份完整「攻防演練技術服務成果報告書」，內容至少應包含測試過程執行之各項細節說明、初測報告、複測報告以及助本府完成弱點漏洞修補說明。	
			小計	15,000,000	0		
小　　計				48,884,286	32,571,428		
合　　計					81,455,714		

（二） 屏東縣政府

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	精進資安防護能量	資訊系統弱點通報機制(VANS)	1,260,000	0	1.完成3個C級機關導入VANS系統。 2.完成3個B級機關導入端點偵測及應變機制(EDR)。	1
			端點偵測及應變機制(EDR)	8,162,222	0		
小　　計				9,422,222	0		
合　　計					9,422,222		

年度	項	工作	工作內容	所需經費	績效	優

	次	項目		經常門	資本門	目標	先次序
113	1	精進資安防護能量	端點偵測及應變機制(EDR)	8,003,444	0	1.完成3個B級機關提交EDR至主管機關指定位置提交。	1
小　　計				8,003,444	0		
合　　計				8,003,444			

（三） 澎湖縣政府

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	提升本府資料中心運作能量，推動機房資源整併共用。	1.汰換並擴充虛擬主機環境硬體設備資源。 2.購置虛擬主機環境必要軟體使用授權。 3.購置虛擬儲存軟體空間必要使用授權。 4.改善資料中心基礎設施運作環境。	1,000,000	4,000,000	1.至少增加50臺虛擬主機運作能量。 2.至少增加25TB儲存空間。 3.維持資訊機房運作妥善率達98%以上。	1
	2	精進本府與基層機關整體網路安全防護機制，強化線路整併機關端網路連線監控環境與防禦能力。	1.推動符合資通安全責任等級C級之機關均導入資訊系統弱點通報機制(VANS)。 2.推動符合資通安全責任等級B級之機關均導入端點偵測及應變機制(EDR)。 3.提升主機操作稽	5,815,000		1.至少12個C級之機關均導入資訊系統弱點通報機制(VANS)。 2.至少3個B級之機關均導入端點偵測及應變機制(EDR)。	2

			核機制運作能量。 4.強化本府與線路整併基層機關網路行為監控、分析與防禦能力。			3.增加主機操作行為事件的可追蹤性，加強操作行為管控。 4.至少有65個線路整併基層機關（單位)納入整體網路安全防護體系。 5.強化終端設備網路行為監控、分析、應變與防禦能力至少達2,600臺。	
	3	完備異地備份儲存機制。	購置相關軟體使用授權，強化異地備份儲存能量，確保備份資料週期有效完整。	1,800,000	0	1.維持備份週期(三代)安全有效。 2.及時提供災害還原所需備份資料。	4
小計				8,615,000	4,000,000		
合計					12,615,000		

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	提升本府資料中心運作能量,推動機房資源整併共用。	1.汰換並擴充虛擬主機環境硬體設備資源。 2.購置虛擬主機環境必要軟體使用授權。 3.購置虛擬儲存軟體空間必要使用	1,000,000	5,100,000	1.至少增加50臺虛擬主機運作能量。 2.至少增加40TB儲存空間。 3.維持資訊機房運作妥善	5

			授權。 4.改善資料中心基礎設施運作環境。			率達 98%以上。	
	2	精進本府與基層機關整體網路安全防護機制，強化線路整併機關端網路連線監控環境與防禦能力。	1.符合資通安全責任等級 B 級之機關依資通安全管理法主管機關指定之方式提交端點偵測及應變機制(EDR)偵測資料。 2.持續推動符合資通安全責任等級 B、C 級之機關均導入資訊系統弱點通報機制(VANS)。 3.建立日誌收集管理機制。	7,670,000	3,000,000	1.至少3個B級機符合可提交端點偵測及應變機制(EDR)偵測資料。 2.至少 15 個 B、C 級之機關均導入資訊系統弱點通報機制(VANS)。 3.至少有 65 個機關納入線路負載平衡機制運作。 4.將資訊設備的記錄收集，加速異常事件的關聯分析速度，智慧化分析事件紀錄與關聯勾稽，及早發現潛在資安威脅與風險，提前預防及告警。	6
小計				8,670,000	8,100,000		
合計					16,770,000		

（四） 臺東縣政府

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	精進資安防護能量	資訊系統弱點通報機制(VANS)	5,350,000	0	1. 至少完成2個C級機關導入VANS系統（含通訊費）。 2. 建置VANS及EDR系統中控主機。 3. 至少完成2個B機關及2個C級機關導入EDR（含通訊費）。	1
			VANS系統及EDR系統超融合運算儲存叢集主機	0	3,080,000		
			端點偵測及應變機制(EDR)	10,404,000	0		
小　　計				15,754,000	3,080,000		
合　　計				18,834,000			

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	精進資安防護能量	端點偵測及應變機制(EDR)	16,656,000	0	至少完成2個B級機關及2個C級機關提交EDR至主管機關指定位置提交（含通訊費）	1
小　　計				16,656,000	0		
合　　計				16,656,000			

九、 經費補助表

（一） 高雄市政府

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	70,577,143	0	21,173,143	49,404,000
113年	81,455,714	0	24,436,714	57,019,000

（二） 屏東縣政府

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	9,422,222	0	942,222	8,480,000
113 年	8,003,444	0	800,344	7,203,100

（三） 澎湖縣政府

單位：新臺幣元

年度	總經費 **（補至千位數）**	其他基金或補助款	地方政府自籌款	行政院補助款
112 年	12,615,000	0	1,263,100	11,351,900
113 年	16,770,000	0	1,689,200	15,080,800

（四） 臺東縣政府

單位：新臺幣元

年度	總經費 **（補至千位數）**	其他基金或補助款	地方政府自籌款	行政院補助款
112 年	18,834,000	0	1,884,000	16,950,000
113 年	16,656,000	0	1,666,000	14,990,000

（五） 補助經費彙總表

單位：新臺幣元

年度	高雄市政府	屏東縣政府	澎湖縣政府	臺東縣政府	小計
112 年	49,404,000	8,480,000	11,351,900	16,950,000	86,185,900
113 年	57,019,000	7,203,100	15,080,800	14,990,000	94,292,900
合計	106,423,000	15,683,100	26,432,700	31,940,000	
總計	180,478,800				

（六） 總經費彙總表

單位：新臺幣元

年度	高雄市政府	屏東縣政府	澎湖縣政府	臺東縣政府	小計
112 年	70,577,143	9,422,222	12,615,000	18,834,000	111,449,222

113 年	81,455,714	8,003,444	16,770,000	16,656,000	122,886,444
合計	152,032,857	17,425,666	29,385,000	35,490,000	
總計	234,333,523				

十、 預定進度

（一） 高雄市政府

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
112/03	0%	0	完成 112 年度採購規劃前置作業。
112/06	30%	21,173,143	完成 112 年度採購發包作業。
112/09	65%	45,875,143	完成 112 年度相關軟硬體設備安裝交貨。
112/12	100%	70,577,143	完成 112 年度相關軟硬體設備驗收付款及結案。

113/03	0%	0	完成 113 年度採購規劃前置作業。
113/06	30%	24,436,714	完成 113 年度採購發包作業。
113/09	65%	52,946,214	完成 113 年度相關軟硬體設備安裝交貨。
113/12	100%	81,455,714	完成 113 年度相關軟硬體設備驗收付款及結案。

（二） 屏東縣政府

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
112/06	0	0	完成採購作業。
112/12	100%	9,422,222	完成交貨安裝、驗收付款及結案。

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
113/06	0%	0	完成採購作業。
113/12	100%	8,003,444	完成交貨安裝、驗收付款及結案。

（三） 澎湖縣政府

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
112/03	0%	0	完成 112 年度採購規劃前置作業。
112/06	30%	3,784,500	完成 112 年度採購發包作業。
112/09	80%	10,092,000	辦理 112 年度相關軟硬體設備安裝測試。
112/12	100%	12,615,000	1. 完成 112 年度相關軟硬體設備安裝交貨。 2. 完成 112 年度相關軟硬體設備驗收付款及結案。

113/03	0%	0	完成 113 年度採購規劃前置作業。
113/06	30%	5,031,000	完成 113 年度採購發包作業。
113/09	80%	13,416,000	辦理 113 年度相關軟硬體設備安裝測試。
113/12	100%	16,770,000	1. 完成 113 年度相關軟硬體設備安裝交貨。 2. 完成 113 年度相關軟硬體設備驗收付款及結案。

（四） 臺東縣政府

時程	累計預定進度(%)	累計預定支用費用(元)	辦理事項
112/06	50%	0	1. 完成採購規劃前置作業 2. 完成採購發包作業
112/12	100%	18,834,000	1. 完成相關軟硬體設備安裝交貨 2. 完成相關軟硬體設備驗收付款及結案

113/06	50%	0	1. 完成採購規劃前置作業 2. 完成採購發包作業

113/12	100%	16,656,000	1. 完成相關軟硬體設備安裝交貨 2. 完成相關軟硬體設備驗收付款及結案

十一、 預期效益

（一） 高雄市政府

1. 資訊資源向上集中

(1) 為配合中央達成「台灣 2030 包容、創新、永續」之智慧國家目標，本府致力於資料中心資源共有、共享之基礎環境創新優化，建立資訊高效能、高可用的資源共享平台整合機制。因此，藉由資料中心的成立並完備雙活機房，拋磚引玉，減少機房之維運成本，達到節能減碳之目標。

(2) 更藉由此主軸延伸，全面提升網路、系統、備份、備援等相關基礎設施，確保異地備份、異地備援資料存放周期有效及安全性，因應災害發生時，能確實有效快速的還原備份資料或切換至異地備援系統，以維持各項系統服務正常運作，營造優質之資訊服務環境。

(3) 資訊資源向上集中化，建立備援機房，使提高共用資源可靠性，可用性，避免服務中斷造成影響。

(4) 資訊資源向上集中後，對於系統主機各項操作行為可以予以紀錄監控，確保資料存取可歸責性及不可否認性，有利後續辦理相關稽核作業。

2. 精進資安防護能量

(1) 導入 VANS：資通安全責任等級 C 級機關政府機關導入資安弱點通報機制（VANS)，藉由安裝弱點通報系統，自動比對軟體資產之弱點，以利執行軟體資產盤點作業(CPE)，落實資訊安全政策，掌握關鍵資訊系統之潛在弱點(CVE)情況，有效評估風險等級之現況與受影響之範圍，確認弱點修補之狀況，並透過系統自動化方式修正相關弱點。

(2) 導入端點偵測及應變機制(EDR):即時針對異常網路行為進行告警與鑑識分析，對於異常網路行為進行應變與攔阻，強化對潛伏惡意程式、資料竊取攻擊、指令與控制等威脅的檢測

與分析能力，降低機關遭入侵成功的風險；並依資通安全管理法主管機關指定之方式提交端點偵測及應變機制(EDR)偵測資料。

3. 推動紅藍軍攻防演練

以紅藍軍攻防演練，找出本府潛在網路環境或系統的漏洞與途徑，並進行後續弱點漏洞修補，同時驗證本府的偵測監控、緊急應變、採證鑑識能力。

（二） 屏東縣政府

1. 導入資通安全責任等級 B、C 級機關政府機關資安弱點通報機制（VANS)，藉由安裝軟體資產管理系統，自動比對軟體資產之弱點，以利執行軟體資產盤點作業(CPE)，掌握關鍵資訊系統之潛在弱點(CVE)情況，有效評估風險等級之現況與受影響之範圍，確認弱點修補之狀況，並透過系統自動化方式修正相關弱點。
2. 導入資通安全責任等級 B 級機關端點偵測及應變機制(EDR)，自動檢測攻擊、快速調查與回應，降低遭受成功攻擊的風險。

（三） 澎湖縣政府

1. 有效運用本府資料中心整體資源，逐步收納所屬機關自設之主機設備，減省機房分散建置的重複投資成本，且資安防護等級具一致性，資源有效向上集中，且具備以下效益：
   （1） 各機關（單位）資訊系統設備採集中式管理，至少可收納本府 11 個單位、所屬一級 5 個機關（不含警察局、消防局、稅務局等 3 個具大型資訊系統及 24 小時受理報案、緊急事件救援、救護性質機關除外）的資通訊系統設備，使各機關（單位）資訊系統設備設置於本府高安全性的資料中心環境中，以提供穩定且優質的縣政資訊服務。
   （2） 各單位使用之資通訊系統設備（含伺服器、儲存設備、網路設備等）由原需 150 臺減少至 25 臺以內，設備減量至少達 80%（125 臺）以上。
   （3） 因應未來系統主機新設及資料未來三年成長需求，擴增資訊中心虛擬主機運作能量，提高設備減量至少達 90%（175

臺）以上。

（4）提高硬體設備運作資源使用率，充分運用硬體設備資源至35%至45%，發揮硬體設備既有效能。

2. 符合資通安全責任等級C級之機關均導入資訊系統弱點通報機制(VANS)，藉由通報平臺系統自動比對軟體資產之弱點，以利執行軟體資產盤點作業(CPE)，落實掌握關鍵資訊系統之潛在弱點(CVE)情況。

3. 符合資通安全責任等級B級之機關均導入端點偵測及應變機制(EDR)，即時針對異常網路行為進行告警與鑑識分析，對於異常網路行為進行應變與攔阻，降低機關遭入侵成功的風險；並依資通安全管理法主管機關指定之方式提交端點偵測及應變機制(EDR)偵測資料。

4. 至少有65個基層機關（單位）對外線路整併集中至縣府統一出口，可協助基層機關（單位）掌控資通訊安全狀態及風險等級，並提供必要的技術支援，以持續性管理及控制基層機關資安風險，避免基層機關（單位）因網路集中整併後，端點設備監測及防禦能力不足，造成整體網路防護的破口。

5. 建立完善且具標準、格式化的日誌管理紀錄機制，快速有效的對於設備事件資訊予以處理分析，便於監控與針對可疑事件採取相關防護作為。

6. 對於系統主機各項操作行為予以紀錄監控，確保資料存取可歸責性及不可否認性，有利後續辦理相關稽核作業。

7. 確保異地備份資料存放周期有效及安全性，因應災害發生時，能確實有效快速的還原備份資料，維持各項系統服務正常運作。

（四） 臺東縣政府

1. 加強及擴大資安弱點通報、端點偵測及應變機制之範圍，另逐步規劃將本縣全體之機關單位納入該範疇，提升本府整體資安防禦量能。

十二、相關聯絡資料

機關單位	姓名	電話	E-mail
高雄市政府 資訊中心基礎設施科	盧漢信	07-799-5678#1318 傳真 07-790-4001	jason41@kcg.gov.tw
屏東縣政府 資訊中心基礎設施科	羅鎮洋管理師	08-732-0415#6335 傳真 08-733-8173	a001627@oa.pthg.gov.tw
澎湖縣政府 行政處資訊科	陳富宗 科長	06-927-4400#314 傳真 06-927-9134	penghu1001@mail.penghu.gov.tw
澎湖縣政府 行政處資訊科	沙潤豪 設計師	06-927-4400#211 傳真 06-927-9134	fa03350@mail.penghu.gov.tw
澎湖縣政府 行政處資訊科	陳蕙芝	06-927-4400#293	amychen@mail.penghu.gov.tw
臺東縣政府 國際發展及計畫處 資訊發展科	余國順	089-340-785 傳真 089-351-965	j3013@taitung.gov.tw
臺東縣政府 國際發展及計畫處 資訊發展科	許筑珺	089-340-785 傳真 089-351-965	l1050@taitung.gov.tw