政府科技發展中程個案計畫書

審議編號：108-3601-06-20-02

行政院資通安全處

「強化政府基層機關資安防護及區域聯防計畫(3/4)

-內政部、財政部、各直轄市政府」

計畫全程：106 年 09 月至 109 年 12 月

108 年 3 月

108-109 年度前瞻基礎建設計畫書修正對照表

計畫名稱：強化政府基層機關資安防護及區域聯防計畫
申請機關(單位)：行政院資通安全處

序號	審查意見/計畫修正前	計畫修正後(說明)	修正處頁碼
1	強化政府基層機關資安防護及區域聯防計畫：P.1-4之主要績效指標(KPI) 部分更新成具量化值(如果有量化值則替換,如果僅有質化值則保留原敘述)(以P.1-7 或 P.8 量化值為更新依據即可)	強化政府基層機關資安防護及區域聯防計畫：P.1-4之最終效益調整為 MSEP 版本,主要績效指標(KPI) 第二點及第四點加入量化值，第一點加入質化值。	4
2	採用設備應有“後門”防漏地檢視機制。	有關設備資安檢設機制，國家通訊傳播委員會（NCC）及經濟部自今（107）年推動物聯網設備資安檢測機制(如 IP CAM、Wi-Fi AP、無線路由器等)，包含資通安全檢測技術指引草案及實驗室認證制度，現已有檢測 IP CAM 產品實驗室，未來持續擴增認證範圍至其他資訊設備。於計畫第 2 期，建議機關採購之設備應送至實驗室進行檢測。	
3	本計畫主責「強化政府基層機關資安防護及區域聯防」,並配合 ISMS 作業規範建立伺服器及資安網路,建議主政單位不定時安排實地訪視,了解實務運作問題與成效。 2. 本計畫於 107 年度因補助規格等問題導致時程延誤，建議主政單位於第	為了解各縣市政府實際執行狀況，除請各地方政府每月提報執行進度外，本院資安處於 107 年 8 月完成期中實地訪查作業，於 108 年將邀集計畫執行部會說明第二期計畫預計執行方式、階段性分配預算、預計執行目標等年度規劃，確保其可行性並具	

	二期計畫適時調整採購程序與落實補助機制。	體落實，亦請各部會定期回報進度說明，並視需要安排實地訪查，以利掌握計畫推動情形。	
4	本計畫第二期預期盤點與汰換老舊 XP 電腦，強化基層機關資安防護，完備國家資安基礎建設，惟現有各縣市單位提出「防毒軟體」服務規格與架構皆不同，建議主政單位採統一規格進行，以利後續管理與維護。	有關委員建議服務規格與架構統一化，查各地方政府防毒軟體係就各縣府實務資安防護需求，依「政府採購法」辦理採購，至於針對委員建議「防毒軟體」之管理與維護，除各地方政府皆有相關管理維護機制外，本院資通安全會報技術服務中心已設置「漏洞公告」，定期要求各機關更新設備漏洞。	
5	本計畫預期強化基層機關資安防護，參與縣市政府將更換諸多硬體設備，建議主政單位審視設備年限管理資料，並落實資訊安全設備採購規範。	本院資安處已請各機關提報計畫時，須檢具「設備汰換清單」，包含財產編號、規格、年限及聯絡人，以審視設備年限管理資料，並落實資訊安全設備採購規範。明年度於實地訪視過程中，將抽測汰換之設備年限是否已達規定以及購置設備是否實際運作。	

第一部分目錄

第一部分

壹、政府科技發展計畫基本資料及概述表(A003)

<table>
<tr><td>審議編號</td><td colspan="5">108-3601-06-20-02</td></tr>
<tr><td>計畫名稱</td><td colspan="5">強化政府基層機關資安防護及區域聯防計畫(3/4)</td></tr>
<tr><td>申請機關</td><td colspan="5">行政院資通安全處</td></tr>
<tr><td>預定執行機關
(單位或機構)</td><td colspan="5">內政部、財政部、行政院資通安全處</td></tr>
<tr><td rowspan="3">預定計畫主持人</td><td>姓名</td><td>簡宏偉</td><td>職稱</td><td colspan="2">處長</td></tr>
<tr><td>服務機關</td><td colspan="4">行政院資通安全處</td></tr>
<tr><td>電話</td><td>(02)3356-8118</td><td>電子郵件</td><td colspan="2">howard@ey.gov.tw</td></tr>
<tr><td>計畫類別</td><td colspan="5">☐一般科技施政計畫
☐新興重點政策計畫
☐延續重點政策計畫
■前瞻基礎建設計畫</td></tr>
<tr><td>跨部會署計畫</td><td colspan="5">■是　☐否</td></tr>
<tr><td>額度</td><td colspan="5">■108年度前瞻基礎建設額度908,000千元
■109年度前瞻基礎建設額度865,599千元</td></tr>
<tr><td>重點政策項目</td><td colspan="5">☐亞洲・矽谷　☐智慧機械　☐綠能產業
☐生技醫藥　■國防產業(資安、微衛星)　☐新農業
☐循環經濟圈　☐晶片設計與半導體前瞻科技
☐數位經濟與服務業科技創新　☐文化創意產業科技創新
☐其他_____</td></tr>
<tr><td>前瞻項目</td><td colspan="5">☐綠能建設　■數位建設　☐人才培育促進就業之建設</td></tr>
<tr><td>計畫群組及比重</td><td colspan="5">生命科技___%　環境科技___%　資通電子___%
工程科技___%　人社科服___%　科技政策 100%</td></tr>
<tr><td>執行期間</td><td colspan="5">108 年 01 月 01 日 至 109 年 12 月 31 日</td></tr>
<tr><td>全程期間</td><td colspan="5">106 年 09 月 13 日 至 109 年 12 月 31 日</td></tr>
<tr><td>中英文關鍵詞</td><td colspan="5">政府組態基準、資訊分享與分析中心、電腦緊急事故處理小組、資安監控中心
Government Configuration Baseline、Information Sharing and Analysis Center、Computer Emergency Response Team、Security Operation Center</td></tr>
<tr><td rowspan="8">資源投入</td><td>年度</td><td colspan="2">經費(千元)</td><td colspan="2">人力(人/年)</td></tr>
<tr><td>106</td><td colspan="2">100,000</td><td colspan="2">63</td></tr>
<tr><td>107</td><td colspan="2">1,573,158</td><td colspan="2">63</td></tr>
<tr><td>108</td><td colspan="2">908,000</td><td colspan="2">75</td></tr>
<tr><td>109</td><td colspan="2">865,599</td><td colspan="2">63</td></tr>
<tr><td>合計</td><td colspan="2">3,446,757</td><td colspan="2">264</td></tr>
<tr><td>108 年度</td><td>人事費</td><td></td><td>土地建築</td><td></td></tr>
</table>

<table>
<tr><td rowspan="10"></td><td rowspan="5"></td><td>材料費</td><td></td><td>儀器設備</td><td></td></tr>
<tr><td>其他經常支出</td><td>166,822</td><td>其他資本支出</td><td>741,178</td></tr>
<tr><td>經常門小計</td><td>166,822</td><td>資本門小計</td><td>741,178</td></tr>
<tr><td colspan="2">經費小計(千元)</td><td colspan="2">908,000</td></tr>
<tr><td rowspan="5">109 年度</td><td>人事費</td><td></td><td>土地建築</td><td></td></tr>
<tr><td>材料費</td><td></td><td>儀器設備</td><td></td></tr>
<tr><td>其他經常支出</td><td>246,191</td><td>其他資本支出</td><td>619,408</td></tr>
<tr><td>經常門小計</td><td>246,191</td><td>資本門小計</td><td>619,408</td></tr>
<tr><td colspan="2">經費小計(千元)</td><td colspan="2">865,599</td></tr>
<tr><td>政策依據</td><td colspan="5">1.FIDP-20170201020000：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-20170503000000：國家資通安全發展方案(106 年至 109 年)：5.3 建構地方政府資安區域聯防體系</td></tr>
<tr><td>與國家科學技術發展計畫關聯</td><td colspan="5">1.NSTP-20170206010000：國家科學技術發展計畫(民國 106 年至 109 年)：1.研發新興資安技術
2.NSTP-20170206020000：國家科學技術發展計畫(民國 106 年至 109 年)：2.發展我國資安科技與應用服務</td></tr>
<tr><td>中程施政計畫關鍵策略目標</td><td colspan="5">1.FIDP-20170201020000：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</td></tr>
<tr><td>本計畫在機關施政項目之定位及功能</td><td colspan="5">我國政府資通安全政策已推行多年，地方政府囿於經費、人力，致使部分機關長年使用已無原廠維護或無法更新之個人電腦或作業系統，儼然成為政府整體資安防護之潛藏風險，尤其在勒索軟體肆虐的今日，此問題更顯嚴峻，爰本計畫，優先強化戶政、役政、地政、警政、衛政、社政及基層公所之資通安全防護，以期建立安全、可信賴的資訊作業環境。另考量六都積極推動電子化政府及智慧城市之際，在各項基礎建設及應用服務（智慧交通、智慧健康、智慧安控、智慧能源、智慧建築、智慧政府及智慧創新）之佈建上，已對鄰近縣市具有帶動與引導作用，而資安防護更是推動電子化政府或智慧城市不可或缺之基礎建設，各縣市如能在各自已建置之資安建設基礎之上，透過區域資安聯防及服務整合，建立地方聯合資訊安全防護網，將有助提升電子化政府與智慧城市之資安應變與防護能量。</td></tr>
<tr><td>計畫重點描述</td><td colspan="5">一、內政部
(一) 汰換縣市工作站及便民服務設備，提升戶、役政資訊系統與地政資訊系統之關鍵基礎設施。
(二) 汰換縣市網路及資安設備，降低機關用戶端及遭入侵之風險。
(三) 導入資安管制軟體及控管機制，簡化管理複雜度，有效控管資安風險。
(四) 建置警政署與重點署屬機關電腦端點資安防護架構，深化情資分享及資安聯防機制，藉此培育資安健診、滲透測試、弱點掃描等資安防護人才，增進警政資安自主能量。
(五) 透過導入專業顧問，成立解決問題導向之團隊，持續針對新型態網路犯罪提供相關建議及諮詢。
二、財政部</td></tr>
</table>

<table>
<tr><td></td><td>(一) 汰換（含擴充或更新）基層機關超過 7 年以上或廠商已停產之資訊軟硬體設備、強化政府財稅機關之資安端點防護及導入政府組態基準。
(二) 強化國庫、關務、國產及賦稅（含國稅及地方稅）等共用資訊系統及軟硬體平臺，提供政府機關安全之資訊作業環境。
三、院資安處
(一) 導入政府組態基準，汰換 7 年以上或已無原廠維護之資訊軟硬體設備，以強化政府基層機關(衛政、社政、基層公所)資安端點防護，完備縱深防禦。
(二) 以六都為核心，結合周邊鄰近縣市推動資安區域聯防，建立中央與地方聯合資訊安全防護網，並帶動地方政府與鄰近學研機構合作，共同培育政府與學界之資安人才。</td></tr>
<tr><td>最終效益
(end-point)</td><td>一、強化基層機關資安防護，完備國家資安基礎建設。
二、透過地方政府區域聯防，提升地方政府資安預警與應處能量。
三、提升國內資安自主產品使用。</td></tr>
<tr><td>主要績效指標
(限填 5 項)
(KPI)</td><td>一、建構區域聯防體系
1.精進資安情資分享機制及內容。
2.建立資安事件區域應變團隊及流程。
3.精進資安監控機制之區域威脅與弱點分析機制，完備地方政府區域資安監控與威脅分析，建構中央與地方之資安聯防體系。
二、導入政府組態基準
1.A、B 等級以上機關優先導入，109 年 A 級機關達 100%，B 級機關達 95%。
2.C 級機關逐年導入。
三、完善基礎資安環境
1.完成各機關之線路整併。
2.逐年汰換機層機關高風險之資訊設備。
四、促進產學研合作
1. 使用國內自主產品，達到使用國內自主研發資安產品之比例 108 年 25%，109 年 50%。
2.推薦我國資安產品每年至少 1 項。
3.提供產學研合作場域。</td></tr>
<tr><td>前一年計畫或相關聯之前期計畫名稱</td><td>全新的新興計畫，無相關前年（或前期）計畫</td></tr>
<tr><td rowspan="3">計畫連絡人</td><td>姓名</td><td>李宗寰</td><td>職稱</td><td>分析師</td></tr>
<tr><td>服務機關</td><td colspan="3">行政院資通安全處</td></tr>
<tr><td>電話</td><td>(02)3356-8061</td><td>電子郵件</td><td>involute@ey.gov.tw</td></tr>
</table>

分年度里程碑：

1. 106 年：實施行政院資安處、內政部及財政部補助地方政府強化資通安全防護作業要點。
2. 107 年：
   (1) 完備直轄市及縣市政府資安防禦藍圖與實際部署（包含資安防護範圍、資安偵測架構、SOC 維運平台等）。
   (2) 建置六都直轄市協同鄰近縣市之區域資安資訊分享及分析平臺。
   (3) 達到使用國內自主研發資安產品之比例 10%。
3. 108 年：
   (1) 完備地方政府區域緊急應變 SOP，確保資訊即時傳遞，啟動區域協防機制。
   (2) 結合資安旗艦計畫及本計畫產出之中央與地方政府資安聯防情資至國家資安資訊分享與分析中心(N-ISAC)，產出國家整體資安情勢。
   (3) 建立地方政府區域聯防檢測機制及軟硬體設備安全評估機制。
   (4) 達到使用國內自主研發資安產品之比例 25%。
4. 109 年：
   (1)完備地方政府區域資安監控與威脅分析，建構中央與地方之資安聯防體系。
   (2)達到使用國內自主研發資安產品之比例 50%，促進我國資安產業發展。

最終效益與里程碑之委員審查意見

**填寫完之表格呈現內容有誤，請修正。

- 「更新」與「新增」之項目符合本計畫政策目標。
- 最終效益 3 「提升國內資安自主產品使用」僅於 109 里程碑中實現，其餘各年里程碑中闕如，請確認是否合宜。**(已於計畫中明訂 106-109 年逐年應達到使用國內自主研發資安產品之比例，107 至 109 年 KPI 目標值分別為 10%、25%及 50%，並列入里程碑)**
- 本案結合資安處其他計畫運作，以強化國內整體資安防護與資安產業推動。建議於最終效益或里程碑中宜有跨計畫結合之論述，以利整合效益評估。**(更新於 108 年里程碑之(2))**

**中程個案計畫書中所條列之主要績效指標宜修正成「可被檢視之效益指標」，並明確告知參與本案之各部會需達成之效益指標。

同意回覆之修正事項

貳、預期效益、主要績效指標(KPI)及目標值

主要績效指標表(KPI)(B003)

屬性	績效指標	106 年實際達成值	107 年度目標值	初級產出量化值		預期效益說明
				108 年度	109 年度	108-109 年度
其他效益(科技政策管理及其他)	其他	100%	-	-	-	研擬行政院補助地方政府強化資通安全防護作業要點
		-	100%	-	-	資訊分享機制：107 年建置、108 及 109 年精進
		-	-	100%	-	緊急應變機制(銜接衛政、社政)：107-108 年建置、109 年精進
		-	-	-	100%	資安監控機制：107、108 年規劃建置、109 年完備
		-	50%	75%	80%	區域聯防涵蓋範圍(%) (機關數/區域直轄市、縣市轄下機關數)
		-	A 級 75% B 級 60%	A 級 95% B 級 80%	A 級 100% B 級 95%	導入機關比例(%)=（導入機關數)/(機關所屬局處數)
		-	80%	100%	100%	符合管理面、技術面、認知與訓練面之應辦事項符合比例(%)=(符合項數/應辦理項數)
		-	1 項	1 項	1 項	實測推薦我國資安優質產品 (項)
		-	100%	100%	100%	個人 PC 採購國內自主產品
		-	10%	25%	50%	其他設備採購國內自主產品

參、人力配置/經費需求/經費分攤

人力需求及配置表(B004)

一、行政院資通安全處

分項人力需求及配置說明

1.本計畫並無編列人事相關費用，計畫之整體規劃與執行將由本處既有組織編制依業務統籌分工辦理。

2.本計畫補助各直轄市、縣(市)政府，將依「行政院補助地方政府強化資通安全防護作業要點」辦理。地方政府人力依各直轄市、縣(市)政府現有組織架構及人員辦理，不另新增人力。

單位：人/年

計畫名稱	108 年度							109 年度	110 年度	111 年度
	總人力	職級						總人力	總人力	總人力
		研究員級(含)以上	副研究員級	助理研究員級	研究助理級	技術人員	其他			
強化政府基層機關資安防護及區域聯防計畫	3	2	0	1	0			3	-	-

二、內政部

分項人力需求及配置說明

1.本計畫並無編列人事相關費用，計畫之整體規劃與執行將由內政部既有組織編制依業務統籌分工辦理。

2.戶役政之基層機關資訊設備汰換，將依據「政府採購法」及「行政院所屬各機關資訊業務委外服務作業參考原則」，基於提升營運效率之考量及在能夠有效監督、評估及控制委外服務品質之前提下，辦理委外採購作業。

3. 補助地政基層汰換資訊設備，將依「內政部補助地方政府強化戶役政基層機關資安防護及區域聯防計畫作業要點」辦理。地方政府人力依各直轄市、縣(市)政府現有組織架構及人員辦理，不另新增人力。

4.警政署及所屬機關因業務性質持有大量特種個資，旨在提升警察機關資安防護能量，防止資料外洩，並進行人才培育，強化資安自主能量，計畫將依據「政府採購法」及「行政院所屬各機關資訊業務委外服務作業參考原則」，基於提升營運效率之考量及在能夠有效監督、評估及控制委外服務品質之前提下，辦理委外採購作業。

單位：人/年

計畫名稱	108 年度							109 年度	110 年度
	總人力	職級						總人力	總人力
		研究員級(含)以上	副研究員級	助理研究員級	研究助理級	技術人員	其他		
一、強化政府基層機關資安防護及區域聯防計畫									
(一)內政部(戶役政)之基層資訊設備汰換整體計畫	3	1	1	1				3	-
(二) 內政部(地政)之基層資訊設備汰換整體計畫	47	24	23					47	
(三) 內政部警政署建置電腦端點資安聯防及人才培育計畫	12	7	1	4					

三、財政部

分項人力需求及配置說明

1.本計畫並無編列人事相關費用，計畫之整體規劃與執行將由財政部既有組織編制依業務統籌分工辦理。

2.本計畫將依據「政府採購法」及「行政院所屬各機關資訊業務委外服務作業參考原則」，基於提升營運效率之考量及在能夠有效監督、評估及控制委外服務品質之前提下，辦理委外採購作業。

3. 補助稅政基層汰換資訊設備，將依「財政部補助地方稅稽徵機關強化資通安全防護作業要點」辦理。地方政府人力依各直轄市、縣(市)政府現有組織架構及人員辦理，不另新增人力。

單位：人/年

計畫名稱	108 年度							109 年度	110 年度	111 年度
	總人力	職級						總人力	總人力	總人力
		研究員級(含)以上	副研究員級	助理研究員級	研究助理級	技術人員	其他			
財政部「強化政府基層機關資安防護及區域聯防計畫」	10	6	4	0	0	0	0	10	-	-

經費需求表(B005)

一、行政院資通安全處

分項經費需求說明

本項補助中央部會及六都直轄市，強化資安防護設備、創新服務新系統開發及汰換超過年限(高風險)之資訊設備等。

單位：千元

計畫名稱	計畫目標	計畫性質	108 年度							109 年度			110 年度			111 年度		
			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	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									
強化政府基層機關資安防護計畫及區域聯防計畫	1.全面強化基層機關資安防護，完備國家資安基礎建設。 2.落實六都及縣市政府資安區域聯防。 3.提升國內資安自主產品使用	其他	515,875			159,862			356,013	539,830	246,191	293,639	-	-	-	-	-	-

二、內政部

經費需求說明

補助基層機關(戶役地警政)汰換超過年限(高風險)之資訊設備及強化資安防護設備等。

單位：千元

計畫名稱	計畫目標	計畫性質	108年度							109年度			110年度		
			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
				人事費	材料費	其他費用	土地建築	儀器設備	其他費用						
一、內政部(戶役政)之基層資訊設備汰換整體計畫 二、內政部(地政)之基層資訊設備汰換整體計畫 三、內政部(警政)建置電腦端點資安聯防及人才培育計畫	1.辦理地方政府工作站及周邊設備更新，提升戶役政資訊系統及地政整合系統地籍資料庫關鍵基礎設施。 2.辦理地方政府網路及資安設備更新，提升整體資安防護機制。 3.導入基層機關政府組態基準規範，有效控制電腦遭受駭客入侵，以降低資安事件。 4.建置警政基層機關電腦端點資安防護架構，深化情資分享及資安聯	其他 其他	108,000			6,960			101,000	96,000		96,000	-	-	-

	防機制，藉此培育資安健診、滲透測試、弱點掃描等資安防護人才，增進警政資安自主能量。 5.透過導入專業顧問，成立解決問題導向之團隊，持續針對新型態網路犯罪提供相關建議及諮詢。														

三、財政部

經費需求說明

補助基層機關稅政汰換超過年限(高風險)之資訊設備及強化資安防護設備等。

單位：千元

計畫名稱	計畫目標	計畫性質	108年度							109年度			110年度			111年度		
			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	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									
財政部「強化政府基層機關資安防護及區域聯防計畫」		其他	284,125						284,125	229,769		229,769	-	-	-	-	-	-

經費分攤表(B008)

跨部會 主提 機關 (含單位)	跨部會 申請 機關 (含單位)	計畫名稱	106 年度 法定數(千元)	107 年度 法定數(千元)	108 年度 申請數(千元)	109 年度 申請數(千元)
財政部	本院資安處	強化政府基層機關資安防護及區域聯防計畫-財政部	40,000	368,575	284,125	229,769
內政部	本院資安處	強化政府基層機關資安防護及區域聯防計畫-內政部	0	826,160	108,000	96,000
本院資安處	本院資安處	強化政府基層機關資安防護及區域聯防計畫-本院資安處	60,000	378,423	515,875	539,830
各額度經費合計			100,000	1,573,158	908,000	865,599

肆、 儀器設備需求(如單價 500 萬以上儀器設備需俟補助對象申請通過才採購而暫無法詳列者,嗣後應依規定另送科技部審查)申購單價新臺幣 500 萬元以上科學儀器送審彙總表(B006)

申請機關：　　(單位：新臺幣千元)

年度	編號	儀器名稱	使用單位	數量	單價	總價	優先順序		
							1	2	3
108		無							
總　　計									
109		無							
總　　計									

（主管機關名稱）
申購單價新臺幣 500 萬元以上科學儀器送審表(B007)
中華民國 xxx 年度
(若 108、109 年度分別購置儀器，此表單另請新增)

申請機關(構)	無				
使用部門					
中文儀器名稱					
英文儀器名稱					
數量		預估單價(千元)		總價(千元)	
購置經費來源	■前瞻基礎建設特別預算(計畫名稱：_____)				
期望廠牌					
型式					
製造商國別					

一、儀器需求說明

1.需求本儀器之經常性作業名稱：

2.儀器類別：(醫療診斷用儀器限醫療機構得勾選；公務用儀器係指執行法定職掌業務所需儀器，限政府機關得勾選)

□醫療診斷用儀器　□政府機關公務用儀器　□教學或研究用儀器

3.儀器用途：

4.購置必要性說明：(請詳述購置需求，以免因無法檢視儀器必要性而導致負面審查結果)

二、目前同類儀器(醫療診斷及公務用儀器專用)

1.本儀器是

□新購(申請機構無同類儀器)

□增購(申請機構雖有同類儀器，但已不符或不敷使用)

□汰購(汰舊換新)

2.若為增(汰)購，請將申請機構目前使用之同類儀器名稱、廠牌、型式、購買年份及使用狀況詳列於下：

儀器名稱	型式	廠牌	年份	數量	使用現況

二、目前同類儀器(教學或研究用儀器專用)

1.本儀器是

□新購(申請機構所在區域無同類儀器)

□增購(申請機構所在區域雖有同類儀器，但已不符或不敷使用)

□汰購(汰舊換新)

2.若為增(汰)購，請將申請機構所在區域目前使用之同類儀器名稱、廠牌、型式、購買年份(未知可免填)及使用狀況詳列於下：

儀器名稱	儀器所屬機構名稱	型式	廠牌	年份	數量	使用現況

三、儀器使用計畫

1.請詳述本儀器購買後 5 年內之使用規劃及其預期使用效益。(非醫療診斷用儀器請務必填寫近 5 年可能進行之研究項目或計畫)

(1)使用規劃：

(2)預期使用效益：

2.維護規劃：(請填寫儀器維護方式、預估維護費及經費來源等)

3.請詳述本儀器購買後 5 年內之擴充規劃(含配備升級等)，如儀器為整個系統之一部分，則請填寫系統擴充規劃。

(1)儀器是否為整個系統之一部分？

□否

□是，系統名稱：_____

(2)擴充規劃：

4.儀器使用時數規劃

	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月	總時數
可使用時													

數													
自用時數													
對外開放時數													

(1)可使用時數估算說明：

(2)自用時數估算說明：

(3)對外開放時數及對象預估分析：

四、儀器對外開放計畫

□儀器對外開放，開放規劃如下：(請就管理方式、服務項目、收費標準等詳細說明，開放方式可能包含提供使用者自行檢測及分析、接受委託檢測但由使用者自行分析、接受委託檢測及分析等)

□本儀器為整個系統之一部分，系統已對外開放，開放方式如下：

□不對外開放，理由為：(除醫療診斷用及政府機關公務用儀器外，教學或研究用儀器儀器原則對外開放，如未開放須詳述具體理由)

□醫療診斷用儀器，為醫療機構執行醫療業務專用。

□儀器為政府機關執行法定職掌業務所需，以公務優先。

□教學或研究用儀器，說明：_____

五、儀器規格

請詳述本儀器之功能及規格，諸如靈敏度、精確度及重要特性、重要附件與配合設施，並請附送估價單及規格說明書。

1.詳述功能及規格：

2.估價單(除有特殊原因，原則檢附 3 家估價單)

□僅附送_____家估價單，原因為：_____

六、廠牌選擇與評估

1.如擬購他國產品，請說明其理由。

□國產品

□他國產品，原因為：_____

2.比較可能供應廠牌之型式、性能、購置價格、維護保固、售後服務等優缺點，以及對

本單位之適合性。

	廠牌(一)	廠牌(二)	廠牌(三)	…
比較項目(一)				
比較項目(二)				
比較項目(三)				
比較項目(四)				

七、人員配備與訓練

1.請詳列本儀器購進後使用操作人員簡歷(如有待聘人力，請於姓名欄位註明待聘，餘欄位填列待聘人力之學經歷要求)

姓名	性別	年齡	職稱	學歷	專長	有否受過相關訓練 （請列名稱）

2.使用操作人員進用、調配、訓練規劃(待聘人力須述明進用規劃)

□無

□有，規劃如下：_____

八、儀器置放環境

1.請描述本儀器預定放置場所之環境條件。**(非必要條件，請填無)**

空間大小	平方公尺	相對濕度	%～ %
電壓幅度	伏特～ 伏特	除濕設備	
不斷電裝置		防塵裝置	
溫度	℃～ ℃	輻射防護	
其他			

2.環境改善規劃

□無，預定放置場所已符合儀器所需環境條件。

□有，環境改善規劃及經費來源如下：

(1)擬改善項目包含：_____。

(2)環境改善措施所需經費計_____千元。

(3)環境改善措施經費來源：

□尚待籌措改善經費。

□改善經費已納入本申請案預估總價中。

□改善經費已納入____年度_____預算編列。

九、優先順序

請列出本儀器在機關提出擬購儀器清單中之優先購買順序，並說明其理由。
□第一優先：為順利執行本計畫，建議預算充分支援之儀器項目。
□第二優先：當本計畫預算刪減逾 10%時，得優先減列之儀器項目。
□第三優先：當本計畫預算刪減逾 5%時，得優先減列之儀器項目。
理由說明：_____

伍、108-109 年度前瞻基礎建設計畫自評結果(A007)

一、計畫名稱：強化政府基層機關資安防護及區域聯防計畫

審議編號：108-3601-06-20-02　　原機關計畫編號：

計畫類別：■前瞻基礎建設計畫

二、評審委員：何委員建明、陳委員俊良、孫委員雅麗

日期：　107　年　3　月　5　日

三、計畫概述：本計畫優先強化戶政、役政、地政、警政、衛政、社政及基層公所之資通安全防護，以期建立安全、可信賴的資訊作業環境。另考量六都積極推動電子化政府及智慧城市之際，在各項基礎建設及應用服務（智慧交通、智慧健康、智慧安控、智慧能源、智慧建築、智慧政府及智慧創新）之佈建上，已對鄰近縣市具有帶動與引導作用，而資安防護更是推動電子化政府或智慧城市不可或缺之基礎建設，各縣市如能在各自已建置之資安建設基礎之上，透過區域資安聯防及服務整合，建立地方聯合資訊安全防護網，將有助提升電子化政府與智慧城市之資安應變與防護能量。

四、審查意見：

1. 本案需要先盤點目前地方政府，因個人電腦或伺服器之作業系統老舊而無原廠維護或無法更新的資安問題有多嚴重。
2. 目前國內很多資安公司之軟體由委外/境外開發，資安自主性產品方面需要更精確的定義。
3. 本案「以六都為核心建置地方政府資安區域聯防機制，比率達 100%」的，「區域聯防機制」的定義需要更精確。
4. 配合本計畫執行，應同時建立各戶政事務所之資安防護管理系統。
5. 建議增加 milestone，包括：逐年執行建置對國家安全聯防體系的整體資訊安全提升效益、資安強化重點及程度，並以質化方式敘明。
6. 本案應與建構公教體系綠能雲端資料中心計畫協調，並密切配合介接。

五、本處回應：

1. 初步統計，地方政府及基層機關大約尚存 1 萬 9 千多台無原廠更新之個人電腦(Windows XP)，同時，微軟亦宣布 109 年，將停止 Win7 之安全性更新，本計畫規劃汰換 7 年以上且無原廠維護之電腦主機並導入政府基準組態設定(GCB)，以提升基層機關之執行效率。
2. 資安自主性產品定義之認定須兼顧扶植國內產業、避免阻礙國外投資及市場公平競爭等因素，本處刻與經濟部研議中，將考量市場競爭機制，產品供應鏈、研發、生產及軟體開發等多個面向訂定。
3. 有關區域聯防機制 100%，係指完成以下項目：
   (1) 橫向整合跨部會，跨 SOC 情資，提供威脅情資
   (2) 垂直跨行政區域與層級，提供防護建議
   (3) 資安事件準確通報
   (4) 鉅量長期分析，發掘潛在威脅
   (5) 可疑事件長期追蹤，縮短潛伏風險，降低無形損失
   (6) 早期預警，降低零時差威脅
   (7) 預計 109 年完成以上項目，完成率達 100%。
4. 有關各戶政事務所之資安防護管理系統，目前由內政部「全國戶役政資訊系統集中化建置計畫」及「戶役政綠色便民及資安強化計畫」規劃辦理。

   本計畫係協助汰換戶役政基層機關超過 7 年以上已無原廠維護之電腦主機並導入政府基準組態設定(GCB)。
5. 本計畫將參採委員意見，規劃於 107 年完成 ISAC、108 年完成 CERT、109 年完成 SOC，以建構完整的資安聯防體系，說明如下：
   (1) ISAC：橫向整合跨縣市，跨 SOC 情資，提供威脅情資、垂直跨行政區域與層級，提供防護建議。
   (2) CERT：區域聯防整體防護規劃與應變，其各直轄市及縣市政府之通報方式依「國家資通安全通報應變作業綱要」辦理。
   (3) SOC：鉅量長期分析，發掘潛在威脅、可疑事件長期追蹤，縮短

潛伏風險，降低無形損失、早期預警，降低零時差威脅。

6. 「強化政府基層機關資安防護及區域聯防」主要規劃由內政部、財政部及六都結合鄰近縣市，強化基層機關資安防護。感謝委員建議，未來各工作項目亦將持續配合執行。

陸、中程個案計畫自評檢核表

※ 下表資料填寫完畢後請合併於計畫書中。

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		✓			

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	
	c.請增人力之類別及進用方式 d.請增人力之經費來源					
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：分析師李宗寰　　單位主管　處長簡宏偉　首長

主管部會核章：　　會計主管　　首長

性別影響評估檢視表

※ 下表資料填寫完畢後請轉合併於計畫書中。

【第一部分】：本部分由機關人員填寫

填表日期：　107　年　7　月　18　日			
填表人姓名：李宗寰 電話：02-33568061	職稱：分析師 e-mail：involute@ey.gov.tw		身份：■業務單位人員 □非業務單位人員， (請說明：_____)
填　表　說　明 一、行政院所屬各機關之中長程個案計畫除因物價調整而需修正計畫經費，或僅計畫期程變更外，皆應填具本表。 二、「主管機關」欄請填列中央二級主管機關，「主辦機關」欄請填列擬案機關(單位)。 三、建議各單位於計畫研擬初期，即徵詢性別平等專家學者或各部會性別平等專案小組之意見；計畫研擬完成後，應併同本表送請民間性別平等專家學者進行程序參與，參酌其意見修正計畫內容，並填寫「拾、評估結果」後通知程序參與者。			
壹、計畫名稱	強化政府基層機關資安防護及區域聯防計畫		
貳、主管機關	行政院資通安全處	主辦機關(單位)	行政院資通安全處
參、計畫內容涉及領域：			勾選(可複選)
3-1 權力、決策、影響力領域			
3-2 就業、經濟、福利領域			V
3-3 人口、婚姻、家庭領域			
3-4 教育、文化、媒體領域			
3-5 人身安全、司法領域			
3-6 健康、醫療、照顧領域			
3-7 環境、能源、科技領域			V
3-8 其他(勾選「其他」欄位者，請簡述計畫涉及領域)			

肆、問題與需求評估		
項　目	說　明	備　註
4-1 計畫之現況問題與需求概述	鑒於地方政府投入資通安全相關之經費有限，長年以來資訊軟硬設備難以更新，致使部分個人電腦或作業系統已無原廠維護或無法更新，成為政府整體資安防護之潛藏風險，此外，考量六都積極推動智慧城市之際，在各項基礎建設及應用服務（智慧交通、智慧健康、智慧安控、智慧能源、智慧建築及智慧創新）之佈建上，已對鄰近縣市具有帶動與引導作用，而資安防護更是推動智慧城市不可或缺之基礎建設，然各縣市如能在各自已建置之資安建設基礎之上，透過區域資安聯防及服務整合，建立地方聯合資訊安全防護網，將有助提升智慧城市之資安應變與防護能量。	簡要說明計畫之現況問題與需求。

4-2 和本計畫相關之性別統計與性別分析	本計畫由各執行機關：內政部、財政部及六都直轄市、縣市政府，於本院性別平等會網站之性別統計專區，統計從事資通安全人員及主管之性別比例。 另有關大專以上各級資訊科系相關師生之性別統計，本計畫將參考教育部統計處網站之性別統計指標彙總性資料，瞭解各項指標，查 106 學年度各大專院校共 69,746 位學生，其中男生 29,679、女生 40,067(性別比例符合 1/3)，後續將鼓勵性別平等教育學術研究之發展與教材教法之開發，制定適合各級教育階段各類形式教材，融入性別平等教育相關議題的基本規範或要點。	1.透過相關資料庫、圖書等各種途徑蒐集既有的性別統計與性別分析。 2.性別統計與性別分析應儘量顧及不同性別、性傾向及性別認同者之年齡、族群、地區等面向。
4-3 建議未來需要強化與本計畫相關的性別統計與性別分析及其方法	本計畫將由各執行機關：內政部、財政部及六都直轄市、縣市政府，於本院性別平等會網站之性別統計專區，統計資通安全人才培育及參與人員之性別統計，以作為未來改善性別參與之參據。	說明需要強化的性別統計類別及方法，包括由業務單位釐清性別統計的定義及範圍，向主計單位建議分析項目或編列經費委託調查，並提出確保執行的方法。
伍、計畫目標概述(併同敘明性別目標)	一、 全面強化基層機關資安防護，完備國家資安基礎建設。 二、 落實六都及縣市政府資安區域聯防。 三、 提升國內資安自主產品使用。 四、 本計畫執行過程中，委託維運廠商執行各項工作及研究時，將依性別平等政策綱領之性別平等工作法，落實友善家庭措施之人力資源管理。此外受託單位員工人數如達 30 人以上，亦叮囑受託單位設置職場性騷擾防治專線及窗口。 五、 本計畫之資通安全人才培育，將以鼓勵女性參與，縮短性別落差列為性別目標，各主管部門亦將以積極策略改變教育過程之性別刻板角色複製，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。	
陸、性別參與情形或改善方法(計畫於研擬、決策、發展、執行之過程中，不同性別者之參與機制，如計畫相關組織或機制，性別比例是否達 1/3)	本計畫之研擬、決策過程中參與者（如諮詢的專家學者、說明會、與計畫研擬相關之重要會議參與者）性別統計，共 5 位參與計畫研擬與決策，其中男性 2 位、女性 3 位，另首席評議專家男性 2 位、女性 1 位，符合性別比例 1/3。	

柒、受益對象

1.若 7-1 至 7-3 任一指標評定「是」者，應繼續填列「捌、評估內容」8-1 至 8-9 及「第二部分－程序參與」；如 7-1 至 7-3 皆評定為「否」者，則免填「捌、評估內容」8-1 至 8-9，逕填寫「第二部分－程序參與」，惟若經程序參與後， 10-5「計畫與性別關聯之程度」評定為「有關」者，則需修正第一部分「柒、受益對象」7-1 至 7-3，並補填列「捌、評估內容」8-1 至 8-9。

2.本項不論評定結果為「是」或「否」，皆需填寫評定原因，應有量化或質化說明，不得僅列示「無涉性別」、「與性別無關」或「性別一律平等」。

項　目	評定結果(請勾選)		評定原因	備　註
	是	否		
7-1 以特定性別、性傾向或性別認同者為受益對象		V	本計畫並無特定性別、性傾向或性別認同者為受益	如受益對象以男性或女性為主，或以同性戀、異性戀或雙性戀為主，或個人自認屬於男性或女性者，請評定為「是」。

			對象，惟計畫執行過程，將依性別平等政策綱領之性別平等工作法，落實友善家庭措施之人力資源管理，此外受託單位員工人數如達 30 人以上，亦叮囑受託單位設置職場性騷擾防治專線及窗口。	
7-2 受益對象無區別，但計畫內容涉及一般社會認知既存的性別偏見，或統計資料顯示性別比例差距過大者		V	本計畫之受益對象並未限於特定性別人口群，且無涉及性別偏見或性別比例差距過大之可能性。	如受益對象雖未限於特定性別人口群，但計畫內容涉及性別偏見、性別比例差距或隔離等之可能性者，請評定為「是」。
7-3 公共建設之空間規劃與工程設計涉及對不同性別、性傾向或性別認同者權益相關者		V	本計畫非公共建設之空間規劃，並無涉及性別便利性、區位安全性。	如公共建設之空間規劃與工程設計涉及不同性別、性傾向或性別認同者使用便利及合理性、區位安全性，或消除空間死角，或考慮特殊使用需求者之可能性者，請評定為「是」。

捌、評估內容

(一)資源與過程

項　目	說　明	備　註
8-1 經費配置：計畫如何編列或調整預算配置，以回應性別需求與達成性別目標	無	說明該計畫所編列經費如何針對性別差異，回應性別需求。
8-2 執行策略：計畫如何縮小不同性別、性傾向或性別認同者差異之迫切性與需求性	無	計畫如何設計執行策略，以回應性別需求與達成性別目標。
8-3 宣導傳播：計畫宣導方式如何顧及弱勢性別資訊獲取能力或使用習慣之差異	無	說明傳佈訊息給目標對象所採用的方式，是否針對不同背景的目標對象採取不同傳播方法的設計。
8-4 性別友善措施：搭配其他對不同性別、性傾向或性別認同者之友善措施或方案	無	說明計畫之性別友善措施或方案。

(二)效益評估

項　目	無	備　註
8-5 落實法規政策：計畫符合相關法規政策之情形	無	說明計畫如何落實憲法、法律、性別平等政策綱領、性別主流化政策及 CEDAW 之基本精神，可參考行政院性別平等會網站(http://www.gec.ey.gov.tw/)。

8-6 預防或消除性別隔離：計畫如何預防或消除性別隔離	無	說明計畫如何預防或消除傳統文化對不同性別、性傾向或性別認同者之限制或僵化期待。
8-7 平等取得社會資源：計畫如何提升平等獲取社會資源機會	無	說明計畫如何提供不同性別、性傾向或性別認同者平等機會獲取社會資源，提升其參與社會及公共事務之機會。
8-8 空間與工程效益：軟硬體的公共空間之空間規劃與工程設計，在空間使用性、安全性、友善性上之具體效益	無	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。
8-9 設立考核指標與機制：計畫如何設立性別敏感指標，並且透過制度化的機制，以便監督計畫的影響程度	無	1.為衡量性別目標達成情形，計畫如何訂定相關預期績效指標及評估基準(績效指標，後續請依「行政院所屬各機關個案計畫管制評核作業要點」納入年度管制作業計畫評核)。 2.說明性別敏感指標，並考量不同性別、性傾向或性別認同者之年齡、族群、地區等面向。

玖、評估結果：請填表人依據性別平等專家學者意見之檢視意見提出綜合說明，包括對「第二部分、程序參與」主要意見參採情形、採納意見之計畫調整情形、無法採納意見之理由或替代規劃等。

9-1 評估結果之綜合說明	本計畫最終受益者不分性別，但是在推動執行過程中每一環節均涉及人員及廠商，涉及委外招標時，將要求委外承商接納不同性別的就業族群，推動友善平權就業環境，並於計畫執行期間，定期檢視兩性參與計畫成員比例，落實兩性平權，縮小性別落差。	
9-2 參採情形	9-2-1 說明採納意見後之計畫調整	無
	9-2-2 說明未參採之理由或替代規劃	無
9-3 通知程序參與之專家學者本計畫的評估結果： 已於 106 年 6 月 26 日，完成 106 年度至 109 年度計畫書性評審查。		

【第二部分－程序參與】：本部分由民間性別平等專家學者填寫

<table>
<tr><td colspan="4">拾、程序參與：若採用書面意見的方式，至少應徵詢 1 位以上民間性別平等專家學者意見；民間專家學者資料可至台灣國家婦女館網站參閱(http://www.taiwanwomencenter.org.tw/)。</td></tr>
<tr><td colspan="4">(一)基本資料</td></tr>
<tr><td>10-1 程序參與期程或時間</td><td colspan="3">106 年 6 月 26 日至 106 年 7 月 6 日</td></tr>
<tr><td>10-2 參與者姓名、職稱、服務單位及其專長領域</td><td colspan="3">吳嘉麗　淡江大學化學系榮譽教授/臺北市女性權益委員會委員
性別與科技</td></tr>
<tr><td>10-3 參與方式</td><td colspan="3">□計畫研商會議　□性別平等專案小組　■書面意見</td></tr>
<tr><td rowspan="2">10-4 業務單位所提供之資料</td><td>相關統計資料</td><td>計畫書</td><td>計畫書涵納其他初評結果</td></tr>
<tr><td>□有　□很完整
□可更完整
□現有資料不足須設法補足
■無　□應可設法找尋
□現狀與未來皆有困難</td><td>□有，
且具性別目標
■有，
但無性別目標
□無</td><td>□有，
已很完整
■有，
但仍有改善空間
□無</td></tr>
<tr><td>10-5 計畫與性別關聯之程度</td><td colspan="3">□有關　　■無關
（若性別平等專家學者認為第一部分「柒、受益對象」7-1 至 7-3 任一指標應評定為「是」者，則勾選「有關」；若 7-1 至 7-3 均評定「否」者，則勾選「無關」）。</td></tr>
<tr><td colspan="4">(二)主要意見：就前述各項（問題與需求評估、性別目標、參與機制之設計、資源投入及效益評估）說明之合宜性提出檢視意見，並提供綜合意見。</td></tr>
<tr><td colspan="2">10-6 問題與需求評估說明之合宜性</td><td colspan="2">本計畫可做之性別統計如 1. 六都及縣市政府從事資通安全人員及主管之性別統計　2. 大專以上各級資訊科系相關師生之性別統計以為未來人才進用之來源。
前述 2.可由教育部性別統計網站查得，至於 1 如目前沒有，則可在本計畫執行中進行統計。</td></tr>
<tr><td colspan="2">10-7 性別目標說明之合宜性</td><td colspan="2">推動六都及各縣市政府資安區域聯防之同時可進行各區資安人員性別統計，並提醒相關委員會任一性別人數不得低於 1/3。
本計畫並擬帶動地方政府與鄰近學研機構合作，共同培育政府與學界之資安人才，人才培育尤應提升少數性別之參與機會，設定目標比例，以積極落實縮小性別落差。</td></tr>
<tr><td colspan="2">10-8 性別參與情形或改善方法之合宜性</td><td colspan="2">「針對競標廠商就業人口性別進行評估」不夠明確，建議各競標廠商應將該廠商之各項性別平等措施作為附件參考，例如是否有員工對性侵性騷之申訴管道電話，有無公告，以及其他哺乳設施、生理假、育嬰休假等友善措施。
進行區域性教育訓練時，亦請關注學員及師資之性別比例。</td></tr>
<tr><td colspan="2">10-9 受益對象之合宜性</td><td colspan="2">針對競標廠商如 10-8 建議</td></tr>
<tr><td colspan="2">10-10 資源與過程說明之合宜性</td><td colspan="2">建議落實推動 10-6/10-7/10-8 之建議</td></tr>
<tr><td colspan="2">10-11 效益評估說明之合宜性</td><td colspan="2">本計畫最終受益者不分性別，但是在推動執行過程中每一環節均涉及人員及廠商，如協助推動前述建議，方有助於落實性別主流化。</td></tr>
<tr><td colspan="2">10-12 綜合性檢視意見</td><td colspan="2">本計畫最終受益者不分性別，但是在推動執行過程中每一環節均涉及人員及廠商，原表說明均不夠明確，執行時有相當模糊空間，如協助推動前述建議，方有助於落實性別主流化。</td></tr>
<tr><td colspan="4">(三)參與時機及方式之合宜性　合宜</td></tr>
<tr><td colspan="4">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）　吳嘉麗</td></tr>
</table>

108-109 年度前瞻基礎建設計畫審查意見回復表(A008)

計畫名稱：強化政府基層機關資安防護及區域聯防計畫
申請機關(單位)：行政院資通安全處
一、審查意見回復

序號	審查意見/計畫修正前	意見回復/計畫修正後 (說明)	修正處頁碼
1	資安處宜協助內政部建立協調管理機制，落實執行各計畫工作項目的專案管理，並重新檢視本計畫整體彙整之預期效益(質化+量化)、最終效益(end-point)等，確保整體政策目標之達成。	有關委員建議請本院資安處協助內政部及財政部進行專案管理及達成預期效益一事，目前內政部及財政部已建立各自專案管理機制，本處將再就該 2 部會之計劃管理機制進行檢討，如有不足之處，將再協調改善，另自下半年開始，本處將進行實地訪視，確保各部會計畫如期如質進行。	-
2	資安處宜協助財政部資訊中心規劃 Action Plan，以達到提升國內資通訊自主產品(含資安產品)使用之目標。	針對財政部提升國產品使用之議題，日前已提醒財政部配合辦理，後續將持續追蹤。	-
3	本案宜有專業的諮詢協作機制，協助地方政府落實資安區域聯防體系的建構與運作。	本院國家資通安全會報技術服務中心已針對地方政府為辦理區域聯防之需要，成立團隊提供技術及諮詢服務。	-
4	戶役政及稅政資訊系統內含許多民眾之個人隱密資訊，因此本計畫委外開發資訊系統時宜有以下措施(1)委託單位宜有內部空間，並要求委外單位開發系統人員進駐開發，以防資訊外洩；(2)設立技術審查機制，以確認程式碼及民眾資料於開發過程安全無虞。	本計畫之執行項目未包含戶役政及稅政之委外開發資訊系統，另針對政府機關資通系統開發之委外管理，目前已訂有「政府資訊作業委外安全參考指引」作為政府機關委外管理之參考。另針對近期通過之「資通安全管理法」，本院刻正訂定相關子法，業已將委外管理規定納入。	-
5	資安處宜與六都(臺北市、新北市、桃園市、臺中市、臺南市、高雄市)資訊長成立「機關資安防護及區域聯防」管理委員會，共同擬定執行 6 子計畫之預期效益(質化+量化)、最終效益(end-point)、主要績效指標(一定要量化)等，達成透過中央	本院已定期召開資安長會議，並就區域聯防機制每季召開國家資安資訊分享與分析中心(N-ISAC)技術交流會議，邀請六都資安長或資安人員分別出席。將參考委員建議事項，檢視各縣市政府計畫執行績效。	-

	政府 N-CERT 與區域 CERT 資 56 防及服務整合，建立地方聯合資訊安全防護網，落實資安聯防、通報、跨領域情資分享與緊急應變機制。		
6	本案最終效益與主要績效指標皆不夠明確，未來無法據以評估計畫執行成效，請重新釐訂各計畫之 Milestone 及 End-point Value，以利政策之達成。	本計畫之區域聯防體系 Milestone 及 Endpoint 將參採委員意見調修，朝向逐年完備聯防涵蓋率等方向訂定。	p.5 p.48
7	有關「結合國內產業與民間社群能量，建立國內外公私協防機制」事項，宜有更具體的作法與預期成效。	本計畫著重政府與學校之合作機制建立，主要作法如下: ♦邀請學校參與地方政府辦理之網路攻防演練。 ♦邀請學校協助地方政府辦理資安事件應變，以縮短資安事件處理時效。 ♦學校與地方政府就面臨之資安議題進行學術研討。	-
8	建構區域聯防體系:應具體定義質化與量化之 a) 何謂「精進資安情資分享機制及內容」，ISAC 已於 107 年度建置，要精進什麼機制？內容為何？b)「2.建立資安事件區域應變團隊及流程」，什麼樣的團隊？ 包含哪些單位、應變時間、涵蓋範圍等？c) 「3.精進資安監控機制之區域威脅與弱點分析機制 」要精進區域威脅與弱點分析機制之具體關鍵指標項目與數量及其重要性。	1. 有關區域聯防體系規劃，如下所示： (1)各地方政府之資安情資分享機制規劃於 107 年度建置完成，惟情資分享內容尚未完備，爰 108 年度至 109 年度將持續精進內容包含: ♦建立情資收發之標準作業程序。 ♦情資資料處理之安全管理程序， ♦擴大情資蒐整範圍、情資分享範圍等。 (2)資安事件區域應變團隊目前係規劃透過跨區域地方政府合作，共組應變團隊等方式，達成共享資源與縮短資安事件發生	p.5 p.48

		後應變時間之目標，應變團隊之組成可由機關與學校合作或委外引進產業能量。 (3)精進資安監控機制之區域威脅與弱點分析機制，主要精進面向將著重於擴充監控範圍及資安事件分析技術等。	
9	導入戶(役地)政及稅政之基層機關及A、B 等級機關縣市之數量統計，佔全國總數之比例。	有關 GCB 導入比例調查，本處係以導入機關比例(%)=(導入機關數)/(機關所屬局處數)計算，查技服中心調查 107 年度地方政府機關(構)，目前地方政府導入 GCB 現況(作業系統及瀏覽器)， A 級 75%、B 級 61%、C 級 60%。	-
10	完善基礎資安環境： 完成各機關之線路整併數量統計，佔全國總數之比例。汰換機層機關高風險之資訊設備數量統計，佔全國總數之比例。	有關各機關之線路整併調查，本處係以線路整併比例(%)=(整併單位數)/(府內單位數)計算，針對受補助之直轄市、縣市，查 107 年度線路整併完成率：高雄 70%、基隆 58%、桃園 30%、苗栗縣 30%、新竹市 90%、新竹縣 100%。 另汰換個人電腦預估數量，初步統計，地方政府及基層機關大約尚存 1 萬 9 千多台無原廠更新之個人電腦(Windows XP)。	-
11	本計畫使用國內自主產品之數量統計，佔全國總數之比例。	目前地方機關刻正辦理資通訊軟硬體採購作業中，使用國內自主產品之數量尚在請地方機關陸續統計中，將於完成初步統計結果後提供資料。	-
12	本計畫內容與其他計畫是否有所關聯，以及可與其他計畫作上、中、下游整合或橫向連結之建議（建議於審查系統中以動態查詢，比較相關計畫）。 可加強與其他計畫整合與連結 ，建議作法： 本計畫與資安旗艦計畫宜加強橫向連結與合作，以利配合帶動本土資安科技及產業發展。	本計畫已規劃在國產品採購、標準設備認證產品採購及實驗場域開放等項目與旗艦計畫連結及合作。後續若有任何連結機會亦將持續辦理。	-

13	評述本計畫資源投入之合理性及建議經費，經費刪減理由請務必具體說明： (一) 業務費（含人事費、材料費及其他經常支出） 不合理 ，理由說明： 1.發展 ISAC、CERT、SOC 系統共享服務，降低資本支出。 2.本案經費缺乏具體的估算依據。 (二) 儀器設備費或其他資本支出 不合理 ，理由說明： 1.本案缺乏具體的估算依據，且有議價調降空間。 (三) 其他費用（含土地建築或其他特殊需求） 合理 極力推薦	(一) 業務費編列說明 1.目前在 ISAC 外部情資來源部分，共通性部分，已由 N-ISAC 統一蒐集轉送各 ISAC，各 ISAC 毋須各自蒐集，其他共享服務仍持續與各 ISAC 討論及研究可行性。 2.有關細部經費估算，將更新計畫內容。 (二) 儀器設備費或其他資本支出 1. 查本計畫之設備經費估算，係參考共同供應契約價格訂定。	p.8- p.12
14	為強化政府機關資安端點防護，提升國家資安基礎防護能量，行政院賡續規劃由內政部、財政部及行政院資通安全處辦理戶政、役政、地政、稅政等基層機關及地方政府高風險資訊軟硬體設備汰換，並建立地方區域聯合資訊安全防護網。本計畫配合「國家資通安全發展方案(106 年至 109 年)」，推動相關工作，有其重要性，建議予以支持。	謝謝委員支持，本計畫將遵照委員意見，賡續規劃由內政部、財政部及行政院資通安全處辦理戶政、役政、地政、稅政等基層機關及地方政府高風險資訊軟硬體設備汰換，並建立地方區域聯合資訊安全防護網。另配合本院「國家資通安全發展方案(106 年至 109 年)」，推動相關工作。	-
15	本案擬汰換使用年限超過 7 年以上之個人電腦及資安防護設備，優先採用國產設備。本計畫之戶(役地)政及稅政之基層機關資安提升工作分別由內政部及財政部主辦，另衛政、社政、基層公所資訊設備汰換及區域資安聯防係由六都結合周邊鄰近縣市(包含花東、離島地區)需求各別提出。	本計畫如委員意見所示，汰換使用年限超過 7 年以上之個人電腦及資安防護設備，分別由內政部及財政部彙整戶、役、地政、稅政；另本處彙整衛政、社政及基層公所之需求。	-
16	目前釐定的 KPI 太含糊，與 107 年度執行內容不易區分，也不清楚「精進」的實質內容與延續性。	本計畫之區域聯防體系 Milestone 及 Endpoint，將參採委員意見調修，朝逐年完備聯防涵蓋率等方向調整，另有關「精進」的部分，各地方政府之資安情資分享機制規劃於 107 年度建置完成，惟情資分享內容尚未完備，爰 108 年度至 109 年度將持續精進內容包含：	-

		♦ 建立情資收發之標準作業程序。 ♦ 情資資料處理之安全管理程序。 ♦ 擴大情資蒐整範圍、情資分享範圍等。	
17	本計畫 PMO 執行管控委員會，建議重新界定彼此關鍵資訊基礎設施資安防護及區域聯防計畫之範疇及內容？ 未來那些是委外 RFP 內容為何？ 委外/自建營運及維護？ 未來建立區域資安聯防之關聯規則為何？ 如何提高防護功效？	本計畫尚未成立 PMO 執行管控委員會，有關關鍵資訊基礎設施資安防護及區域聯防計畫之範疇及內容，本院資安處已訂有 ISAC、CERT、SOC 之建置指引，供各建置機關參考，後續將再視需要，精進文件內容。	-
18	本計畫 PMO 執行管控委員會，宜思考機關執行單位若委外採講硬軟體，合約一定要求委外廠商制定服務水準協議 (Service Level Agreement；SLA)：符合本計畫之 KPI 要求之服務品質、水準以及性能等方面達成協議或訂定契約。	如前項所述，另提醒機關辦理採購應要求訂定 SLA 一事，目前工程會所提供之資訊採購契約範本，已將 SLA 訂為契約需求內容，本處後續將此併入地方政府計畫審查建議事項，送請地方政府加強辦理。 至於地方政府究係委外或自建本計畫內容，以目前地方政府之資安人力能量，仍以委外為主，配合資安管理法之施行，地方政府須視自身資安責任等級配置專職或專責人力，所配置之專職或專責人力，仍以做好委外管理為主要工作。	-
19	本計畫應規劃完整的建設藍圖及執行步驟，並精細估算所需建設經費，避免經費濫用卻無法達成整體的資通安全防護效益。	有關本計畫之建設藍圖及執行步驟，係以建構國家資安聯防體系進行規劃，逐步要求各地方政府排定設備汰換順序及導入 GCB、建置區域情資分享等機制，以有效降低風險，即減少弱點所帶來之衝擊，且提高資安聯防效益。	p.46
20	本計畫補助地方政府汰換資訊設備及建立資安防護網計 11 億 3,747 萬 5,000 元，約占第 2 期經費 18 億元之 63%，立法院審查本計畫第 1 期特別預算時，有相關決議:應先建立一套弱點管理提供各地方政府使用。鑒於資通安全管理法業於 107 年 5 月 11 日經立法院審查通	資安弱點管理為資安日常維運之一環，配合資安管理法之施行，已規劃將此納為機關訂定及實施資通安全維護計畫之法規要求事項，此將有助機關落實資安弱點管理。	-

	過，並預計於 6 月中旬由總統公布，爰請行政院資通安全處除將補助資源投入外，應先檢討協助地方政府訂定弱點管理機制。		
21	本計畫截至 107 年 4 月底止仍未執行，主要係地方政府尚未辦理請款作業所致，考量目前執行進度未達預期目標，建議第 2 期經費按第 1 期預算數匡列 16 億 7,315 萬 8,000 元。	有關補助地方政府經費， 查 107 年 5 月，已有基隆市、屏東縣及臺中市，向本院申請補助，共 2,589 萬 2,465 元，本計畫執行率達 10.39%，另已完成採購但尚未向本院申請經費之直轄市、縣市政府，已請前述地方政府加速申請補助程序。	-
22	應強化「聯防運作」，以符合政策目標；弱點分析宜提出資安防護措施，以達成政府基層機關資安防護之施政目標。	有關強化「聯防運作」，本計畫規劃於 107 年完成 ISAC、108 年完成 CERT、109 年完成 SOC，以建構完整的資安聯防體系，另資安弱點分析將配合資安管理法之施行，要求執行機關須完成資通安全維護計畫，以確保基層機關資安防護。	p.5 p.48
23	與「強化國家資安基礎建設計畫」一致，其防護演練宜請獨立資安公司進行攻擊與實際防護測試效果評估；應協調各地方政府執行資安設備或軟體購置與建置應有基本規範，並應進行相關資安攻擊測試。	有關資安攻防演練，每年係由本院國家資通安全會報技術服務中心辦理，以確保各政府機關建置周全(robustness)的資安防護，另配合資安管理法之子法(資安責任等級分級辦法)，分為管理面、技術面、認知與訓練面規範各項應辦事項，促使中央及地方政府執行資安設備或軟體購置與建置應有基本規範。	-
24	本計畫應有明確營運目標，包括 ISAC 應提供即時且完整之資訊內容、CERT 和 SOC 應有完整的標準作業流程及後續營運機制，以及建置完善的稽核制度；資安處兩項計畫倘有涉及縣市業務者，應有良好的聯結機制，以促進跨機構之溝通合作及營運、管考。	有關各項計畫之間的聯結機制，跨機關之溝通合作及營運、管考，依據科技部訂定之「科技發展類前瞻基礎建設計畫績效管考事宜」，本處設有管考機制，另將視需要進行實地訪視，亦將邀請評議專家一同參與	-
25	本案擬汰換使用年限超過 7 年以上之個人電腦及資安防護設備，建議優先採用國產設備。	有關優先採用國產設備，本計畫績效指標以使用國內資安產品達 50%為目標，並每年推薦一項國內優質資安產品。	p.5 p.48

26	本案建構區域聯防體系，應具體釐訂質化與量化運作指標，以確認是否完備聯防之運作。	有關釐訂區域聯防體系之質化與量化運作指標，本計畫規劃於 107 年完成 ISAC、108 年完成 CERT、109 年完成 SOC，以建構完整的資安聯防體系，另區域聯防涵蓋範圍(%) (機關數/區域直轄市、縣市轄下機關數)，預計 107 年度達 50%、108 年度達 75%、109 年度達 80%為目標。	p.5 p.48

二、計畫書檢視意見回復

序號	檢視意見/計畫修正前	意見回復/計畫修正後 (說明)	修正處頁碼
1	本案由內政部、財政部及行政院資安處辦理戶政、役政、地政、稅政等基層機關及地方政府高風險資訊軟硬體設備汰換，並建立地方區域聯合資訊安全防護網。執行單位對資安環境建設已依原規劃執行，並建立各自專案管理機制。建議進行滾動式成效評估，積極鏈結國內外資安技術團隊，強化本案實質效益產出。	1.有關計畫滾動式成效評估部分，將依據科技部訂頒之「科技發展類前瞻基礎建設計畫推動管制作業規定」，每月追蹤執行情形及每季檢討進度（1、2、3 季，第 4 季併年度績效檢討），後續將安排實地訪查，實際了解各執行機關執行成效後，滾動式修正本計畫目標。 2.有關鏈結國內外資安技術團隊，強化實質效益產出部分，本計畫已訂定有促進產學研合作目標，後續將於實地訪視過程中，了解地方政府標竿模式，供地方政府參考及推廣。	-
2	本案於地方政府劃分多個區域建構資安體系，區域的資安防護與資訊交流合宜，惟推動國家級資安聯防體系，宜釐訂明確之運作機制與管理指標、標準作業程序等，以確保聯防之運作完備及達成國家級資安防護之目的。	有關推動國家級資安聯防體系之運作機制與管理指標、標準作業程序等作法，分述如下： 1.本院國家資通安全會報技術服務中心，已訂定各 N-ISAC、N-CERT、N-SOC 建置指引及執行程序，例如：ISAC 情資交換流程、跨領域 ISAC 情資交換流程、資安事件通報流程及跨層級 SOC 運作流程等。 2.後續將於實地訪視過程中，統整機關共同做法後，於前述已建置之相關文件基礎上，提供其他資安聯防之運作與管理程序，供地方政府參考。	-
3	本案由內政部、財政部及行政院資安處辦理戶政、役政、地政、稅政等基層機關及地方政府之高風險資訊軟硬體設備汰換，並建立地方區域聯合資訊安全防護網。執行單位對資安環境建設已依原計畫之規劃執行，並建立各自專案管理機制。此外，本案將透過協同行政院國家資通安全會報技術服務中心，完成國家層級 N-ISAC、N-CERT、N-SOC 機制，以及建置區域 ISAC、CERT、SOC 機制等作業，達到鏈結國內外資安運作，確保聯防運作完備及達成國家級資安防護之目的。	謝謝委員支持，本計畫將遵照委員意見，協同本院國家資通安全會報技術服務中心，完成國家層級 N-ISAC、N-CERT、N-SOC 機制，並建置地方區域聯防禦網，完成以六都直轄市為核心之區域 ISAC、CERT、SOC，達到鏈結國內外資安運作，確保聯防運作完備及達成國家級資安防護之目的。	-

三、性別影響評估檢視回復

序號	檢視意見/計畫修正前	意見回復/計畫修正後 (說明)	修正處頁碼
1	本案主要係強化基層機關資安防護能量，並以六都為核心建置資安區域聯防，提升鄰近縣市、東部及離外島地區之資安防護。其中部分分項計畫將人才培育列為主要執行項目，如「內政部(警政署)建置電腦端點資安聯防及人才培育計畫」分項計畫，因過去「男理工、女人文」性別刻板印象之影響，長期以來女性在科技領域之參與比例較低，爰建議將在人才培育方面，參考性別平等政策綱領「環境、能源與科技篇」將鼓勵女性參與，縮短性別落差列為性別目標，並研議相關策略或做法，納入該計畫本文。	本計畫將遵照委員意見，參考性別平等政策綱領，增加計畫書第二部份「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」之章節內容，如下所示： 1.鼓勵中央與地方各機關發展積極策略，包括：家庭與工作平衡策略，檢討勞動條件與超時工作情形，以吸引更多女性進入資通訊安全領域就業，並鼓勵男性兼顧家庭照顧責任。 2.落實現行勞動基準法、性別工作平等法、就業服務法等法規，強化性別平等與就業歧視審議機制與申訴管道，增加相關勞動檢查及專業人員訓練。同時，加強企業主於性別工作平等、勞工孕產權益、性騷擾防治等重要議題之性別友善態度與認知；並研議相關鼓勵措施，表彰性別友善企業。 3.落實產假、陪產假、育嬰留職停薪、家庭照顧假、彈性上下班及彈性上班地點等措施，並保障回到職場的權益，避免女性及家庭照顧者因家庭照顧而中斷就業或退出勞動市場。 4.落實政府資訊公開透明，如有重大影響之性別政策，將採取積極措施，並透過大眾媒體，以淺顯易懂方式，讓民眾瞭解，而非僅於網路上公布，方能縮小資訊差距，建立性別參與平等。	p.44
2	性別影響評估檢視表4-2「和本計畫相關之性別統計與性別分析」： 請參考專家學者於檢視表 10-6之建議，補強計畫性別統計，如有性別落差較大之情形，並請分析落差原因。	本計畫將遵照委員意見，參考性平專家於檢視表 10-6 所提建議，修改性別影響評估檢視表 4-2，如下所示： 本計畫將由各執行機關：內政部、財政部及六都直轄市、縣市政府，於本院性別平等會網站之性別統計專區，統計從事資通安全人員及主管之性別比例，符合性別比例 1/3。 另有關大專以上各級資訊科系相關師生之性別統計，本計畫將參考教育部統計處網站之性別統計指標彙總性資料，瞭解各項指標，查 106 學年度各大專院校共 69,746 位學生，其中男生 29,679、	p.25

		女生 40,067，符合性別比例 1/3，後續將鼓勵性別平等教育學術研究之發展與教材教法之開發，制定適合各級教育階段各類形式教材，融入性別平等教育相關議題的基本規範或要點。	
3	性別影響評估檢視表 4-3「建議未來需要強化與本計畫相關的性別統計與性別分析及其方法」： 建議建立本案人才培育及參與人員之性別統計，以作為未來改善性別參與之參據。	本計畫將遵照委員意見，由各執行機關：內政部、財政部及六都直轄市、縣市政府，於本院性別平等會網站之性別統計專區，統計資通安全人才培育及參與人員之性別統計，以作為未來改善性別參與之參據。	p.25
4	性別影響評估檢視表第伍項、計畫目標概述（併同敘明性別目標）： 建議在人才培育方面，將鼓勵女性參與，縮短性別落差列為性別目標。	本計畫將遵照委員意見，增加資通安全人才培育，將以鼓勵女性參與，縮短性別落差為目標，各主管部門亦將以積極策略改變教育過程之性別刻板角色複製，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。	p.25
5	性別影響評估檢視表第陸項、性別參與情型或改善方法： 為瞭解不同性別之需求及參與情形，建議補充本計畫研擬、決策過程中參與者（如諮詢的專家學者、說明會、與計畫研擬相關之重要會議參與者）之性別統計。	本計畫將遵照委員意見，增加本計畫研擬、決策過程中參與者（如諮詢的專家學者、說明會、與計畫研擬相關之重要會議參與者）之性別統計，詳述如下：共 5 位參與計畫研擬與決策，其中男性 2 位、女性 3 位，另首席評議專家男性 2 位、女性 1 位，符合性別比例 1/3。	p.25
6	性別影響評估檢視表第捌項、評估內容 請依據性別統計結果重新評定 7-1 至 7-3，並依評估結果填列「捌、評估內容」。	本計畫將遵照委員意見，重新評定 7-1：「以特定性別、性傾向或性別認同者為受益對象」、7-2：「受益對象無區別，但計畫內容涉及一般社會認知既存的性別偏見，或統計資料顯示性別比例差距過大者」、7-3：「公共建設之空間規劃與工程設計涉及對不同性別、性傾向或性別認同者權益相關者之評估結果」。	p.25- p.26

第二部分目錄

第二部分(自行上傳)撰寫說明

第二部分撰寫說明

壹、 計畫緣起

一、 政策依據

鑒於國際資安威脅情勢日趨嚴峻，為提升國家資安防禦能力，爰透過中央機關與地方政府整體資安聯合防禦機制，輔以地方政府單一目的性的資安防護強化作為，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，期藉由實質經費補助，促進資通安全相關軟硬體建設之發展，提升資通安全管理效能，加強資安防護縱深機制，進而健全資安防護網，達成「厚植自我防護能量，保衛數位國家安全」之目標。

二、 擬解決問題之釐清

我國政府資通安全政策已推行多年，由於地方政府經費、人力、管理制度及技術能力不一，致使部分個人電腦或作業系統已無原廠維護或無法更新，成為政府整體資安防護之潛藏風險，尤其在勒索軟體肆虐的今日，此問題更顯其嚴峻，為使中央機關資安防護機制普遍較地方政府積極完備，及配合行政院刻正發展之國家層級資安防護項目：二線監控機制 G-SOC(Government-Security Operation Center)，均有賴中央機關及各級地方政府共同參與，每一環節皆不可輕忽，期能產生最大之資安聯防綜效，爰本計畫優先強化戶政、役政、地政、警政、衛政、社政及基層公所之資通安全防護，協助其建構安全資訊作業環境、推動資安建設，以期建立可信賴的資通安全環境，確保資料、設備及網路系統之安全，保障民眾權益。

此外，考量六都積極推動電子化政府及智慧城市之際，在各項基礎建設及應用服務（智慧交通、智慧健康、智慧安控、智慧能源、智慧建築、

智慧政府及智慧創新）之佈建上，已對鄰近縣市具有帶動與引導作用，而資安防護更是推動電子化政府或智慧城市不可或缺之基礎建設，各縣市如能在各自已建置之資安建設基礎之上，透過區域資安聯防及服務整合，建立地方聯合資訊安全防護網，將有助提升電子化政府與智慧城市之資安應變與防護能量。

三、目前環境需求分析與未來環境預測說明

前揭推動電子化政府係結合第五期電子化政府（106-109 年度中長程計畫）「主動服務及網路參與精進計畫」，引導地方政府電子化發展，縮短城鄉差距，讓好的資訊服務可以擴散至其他縣市政府，減少資源重置浪費，並與優質政府計畫連結，進一步建立中央與地方持續的互動、溝通及發展策略結合，藉由資訊科技帶動服務價值提升、鏈結各機關服務項目，針對服務族群主動且精準提供服務，協助民眾可快速取得政府服務。由中央間及地方與中央之跨機關電子查驗為基礎著手推動各機關進行服務流程改造，由分散各機關的個別服務，邁向跨機關服務流程整合及創新服務，強化地方政府內部橫向連結及效能提升，並以地方與中央政府一體的概念，提供以民為本的數位服務，建議項目如下：

(一) 提升基層機關資訊服務能力，促使其資訊資源及能力與中央同步完成各縣市政府基層機關充實資訊(含資安、防毒)設施，期能與中央同步，強化資訊服務能力。

(二) e 化服務宅配到家，辦理跨機關電子查驗，成立跨機關工作圈，協調地方與中央機關相關計畫與資源，建立跨機關、跨組織計畫執行之合作機制；以民眾出發角度思維，延續主動服務，地方與中央機關流程簡化整合，將地方機關間合作之稅務、戶政、地、警政等跨地方便民服務，提升為全國一致性便民服務。

本計畫與第五期國家資通安全發展方案緊密銜接，該方案規劃以「打造安

全可信賴的數位經濟時代」為願景，以「建構國家資安聯防體系、提升整體資安防護機制、強化資安自主產業發展」為目標，並透過「完備資安基礎環境」、「建構國家資安聯防體系」、「推升資安產業自主能量」、「孕育優質資安人才」等 4 項策略，推動執行各項工作，其中本計畫係落實「建構國家資安聯防體系」之地方政府資安區域聯防，詳述如下：

以內政部、財政部及六都直轄市結合鄰近縣市(包含花東、離外島地區)，強化基層機關資安防護能量(戶政、役政、地政、警政、稅政、衛政、社政及基層公所)，另以六都為核心建置資安區域聯防，提升鄰近縣市、東部及離外島地區之資安防護，辦理方式如下：

(一) 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)，可即時通知所屬鄰近縣市進行預防或增設阻擋規則。

(二) 建立資安快速應變小組：發生重大資安事件時，透過資安快速應變小組，協防所屬鄰近縣市並提供資安諮詢或技術支援。

(三) 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。

(四) 資安監控中心(Security Operation Center，簡稱 SOC)協防能力：彙整所屬鄰近縣市之資安情資，進行綜合分析以掌握可疑惡意行為。

四、本計畫可發揮之加值或槓桿效果

鑒於資通訊科技日益蓬勃發展，如何提供安全、安心、可靠之網際網路使用環境，創新資安服務價值，朝向虛擬整合化資安服務，已成為邁向優質網路社會之關鍵議題。為達成此一目標，本計畫將促成地方政府與在地產學研合作，達到公私部門相互協力，共同維護我國資通安全之重責大任。

另本計畫配合「國家資通安全發展方案(106 年至 109 年)」，推動相關工

作，有其重要性，為強化政府機關資安端點防護，提升國家資安基礎防護能量，本院賡續規劃由內政部、財政部及行政院資通安全處辦理戶政、役政、地政、警政、稅政等基層機關高風險資訊軟硬體設備汰換，並建立地方區域聯合資訊安全防護網。

五、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

本計畫在於著手打造未來 30 年國家發展需要的基礎建設，並配合政府當前重要國家發展政策，有助於我國資安產業發展。目前我國資安產業，欠缺大型實戰攻防場域淬煉，使得臺灣產品深度與成熟度不足，難與國際大廠競爭，透過本計畫之經費投入，提供資安自主產品之淬煉場域，作為我國資安產業進軍國際所需實績、活絡資安投資市場全力拓銷國際。

另資通訊人才培育方面，將參考本院性別平等會頒訂之「性別平等政策綱領」，推動以下措施：

(一) 鼓勵中央與地方各機關發展積極策略，包括：家庭與工作平衡策略，檢討勞動條件與超時工作情形，以吸引更多女性進入資通訊安全領域就業，並鼓勵男性兼顧家庭照顧責任。

(二) 落實現行勞動基準法、性別工作平等法、就業服務法等法規，強化性別平等與就業歧視審議機制與申訴管道，增加相關勞動檢查及專業人員訓練。同時，加強企業主於性別工作平等、勞工孕產權益、性騷擾防治等重要議題之性別友善態度與認知；並研議相關鼓勵措施，表彰性別友善企業。

(三) 落實產假、陪產假、育嬰留職停薪、家庭照顧假、彈性上下班及彈性上班地點等措施，並保障回到職場的權益，避免女性及家庭照顧者因家庭照顧而中斷就業或退出勞動市場。

(四) 落實政府資訊公開透明，如有重大影響之性別政策，將採取積極措

施，並透過大眾媒體，以淺顯易懂方式，讓民眾瞭解，而非僅於網路上公布，方能縮小資訊差距，建立性別參與平等。

貳、計畫目標

一、目標說明

本計畫主要帶動我國資安產業及技術發展等策略，符合數位建設之主軸一(網路安全)：推動資安基礎建設提供網路安心服務，本計畫達成目標如下：

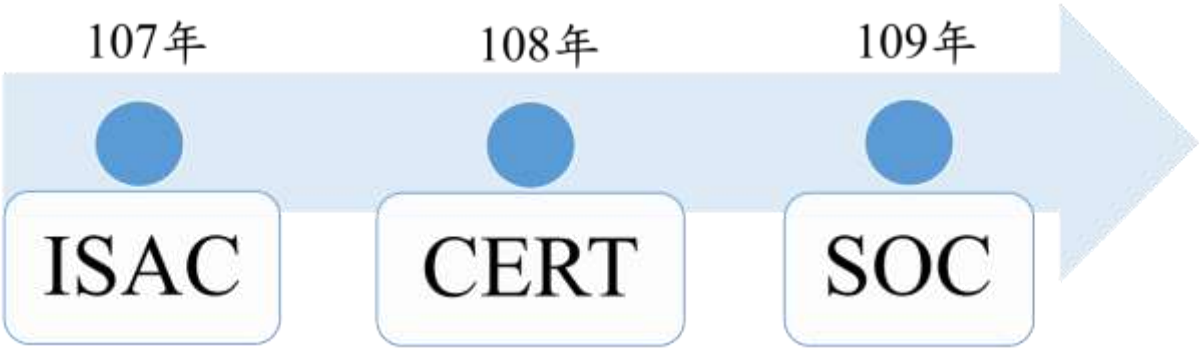
(一) 強化基層機關資安防護，完備國家資安基礎建設之最後一哩。
(二) 透過地方政府區域聯防，提升地方政府資安預警與應處能量。
(三) 提升國內資安自主產品使用。

二、執行策略及方法

(一) 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)，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。
(二) 強化戶政、役政、地政、警政之資安端點防護，以降低基層機關遭入侵之風險，完備縱深防禦。
(三) 以六都為核心，結合周邊鄰近縣市推動資安區域聯防，建立地方聯合資訊安全防護網，並帶動地方政府與臨近學研機構合作，共同培育政府與學界之資安人才。
(四) 汰換軟硬體設備以國內自主資安產品為優先採購標的，推動方式將協調經濟部工業局，優先將國內資安產品納入政府共同供應契約，以提高政府機關採購比例，並由政府發展需求及擴增試驗場域，持續帶動國內資安產業發展。

前述各項重點工作，主要由內政部、財政部及六都直轄市分別執行，詳如附件 1-8。

三、目標實現時間規劃

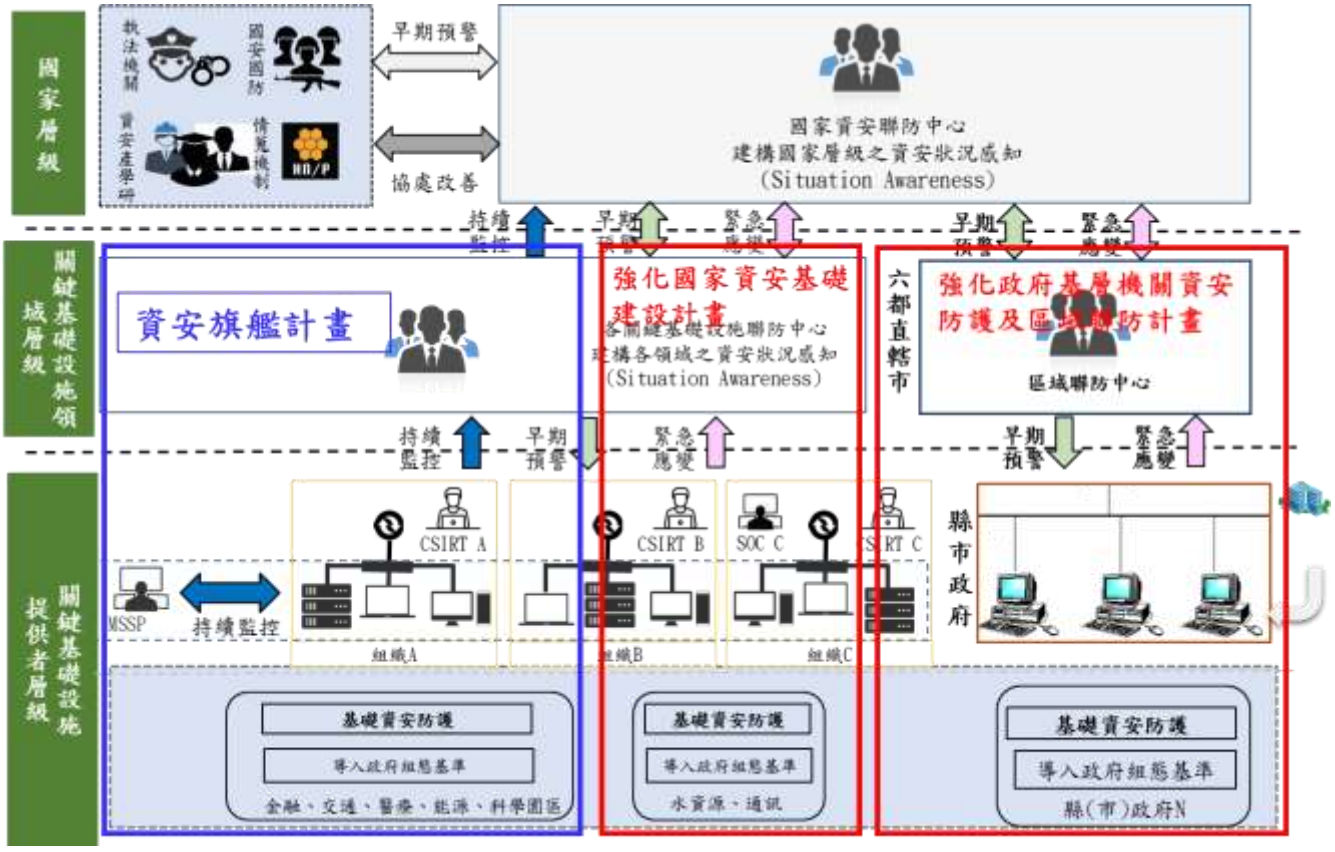


- 107年度各地方政府已配合「政府機關(構)資通安全責任等級分級作業規定」建置各自SOC，但尚未完備且持續營運須投入大量人力及設備經費。
- 本計畫107年係由六都協同鄰近縣市，分年完成區域情資分享機制(ISAC)、108年完成電腦緊急處理小組(CERT)、109年完備區域SOC監控為目標。
- 註：104年度A級機關完成SOC監控、105年度B級機關完成SOC監控。

建構區域聯防體系	導入政府組態基準	完善資安基礎環境	提升資安自主產品使用
• 精進資安情資分享機制及內容 • 建立資安事件區域應變團隊及流程 • 完備資安監控機制之區域威脅與弱點分析機制 • 教育訓練 • 跨縣市合作交流	•GCB分年導入(作業系統、瀏覽器) 108年度達80% • A級95%、B級80%、C級80% •109年度達95% • 109年度：A級100%、B級95%、C級95%	• 符合資通安全管理法子法「資通安全責任等級分級」(管理面、技術面、認知與訓練面)之分級應辦事項	• 推薦及使用國內資安產品，每年1項

四、重要科技關聯圖例

依據本院「國家資通安全發展方案(106年至109年)」發展策略，本計畫與本處另兩項計畫：「強化國家資安基礎建設計畫」及「資安旗艦計畫」，共同落實「建構國家資安聯防體系、提升整體資安防護機制、強化資安自主產業發展」之目標，從風險管理的角度推動國家整體資安防禦工作，完成國家層級ISAC、CERT及SOC之建構，以達資安事件早期預警、持續監控、緊急應變、協處改善之目標，詳如下圖：



參、預期效益、主要績效指標(KPI)及目標值

一、預期效益

1. 導入政府資安防護組態基準(GCB)，汰換基層機關 7 年以上電腦主機及資安防護設備，降低基層機關遭入侵之資安風險，提升政府整體資安防護水準。

2. 以六都為核心建置地方政府資安區域聯防機制，提升地方政府對資安事件之預警與應處能力。
3. 本計畫將以使用國內資安產品達 50%為目標，藉以帶動國內資安產業之發展，進而提升國際競爭力。

二、主要績效指標表(KPI)

施行策略	規範項目	規範內容	107	108	109
建構區域聯防體系	區域聯防體系完備	• 資訊分享機制：107年建置、108及109年精進	100%	-	-
		• 緊急應變機制(銜接衛政、社政)：107-108年建置、109年精進	-	100%	-
		• 資安監控機制：107、108年規劃建置、109年完備	-	-	100%
		• 區域聯防涵蓋範圍(%) (機關數/區域直轄市、縣市轄下機關數)	50%	75%	80%
導入政府組態基準	GCB導入	導入機關比例(%)=（導入機關數)/(機關所屬局處數)	A級75% B級60%	A級95% B級80%	A級100% B級95%
完善資安基礎環境	資通安全管理法子法「資通安全責任等級分級」相關應辦事項	符合管理面、技術面、認知與訓練面之應辦事項符合比例(%)=(符合項數/應辦理項數)	80%	100%	100%
提升資安自主產品使用	自主產品推薦	實測推薦我國資安優質產品(項)	1項	1項	1項
	自主產品使用	個人PC	100%		
		其他設備	10%	25%	50%

三、目標值及評估方法

目標	預算(%)	預期成果效益	績效指標(109 年度)	評估方法	目標值訂定之依據
強化基層機關資安防護，完備國家資安基礎建設之最後一哩	35%	A 級機關全面導入政府組態基準	A 級 100% B 級 95%	導入機關比例(%)	依據 107 年度執行現況評估
透過地方政府區域聯防，提升地方政府資安預警與應處能量	45%	建構地方區域聯防體系	區域聯防涵蓋率 80%	機關涵蓋範圍比例(%)	依據 106 年度至 109 年度 ISAC、CERT、SOC 建置進度評估
提升國內資安自主產品使用	20%	自主產品使用	自主產品使用 50%	基層機關使用產品比例(%)	依據 107 年度國產品使用現況評估

肆、有關機關配合事項及其他相關聯但無合作之計畫

本計畫依據「數位國家‧創新經濟發展方案」之推動主軸一：數位創新基礎環境行動計畫，結合經濟部、交通部、通傳會及國發會等計畫，建立安全可信賴之應用環境，完善我國數位創新基礎環境，並營造一個安全可信賴之數位匯流服務環境。

伍、就涉及公共政策事項，是否適時納入民眾參與機制之說明

本計畫以建置地方政府資安區域聯防及使用國內資安產品達 50%為主要目標，另配合本院國家資通安全會報產業發展組共同推動我國資安產業發展，預估 106 年至 109 年各項科技發展計畫投入資安經費約 110 億元，可促成國內民間業者累計投資額達新臺幣 573 億元，帶動我國 4 年衍生產業關聯效益達新臺幣 1,024 億元。

陸、涉及競爭性計畫之評選機制說明

本計畫之戶、役、地、警政及稅政之基層機關資安提升工作，分別由內政部及財政部主辦，另衛政、社政、基層公所之資訊設備汰換及區域資安聯防係由六都結合周邊鄰近縣市(包含花東、離島地區)需求各別提出，以競爭性為原則，視各六都提報之計畫涵蓋範圍而定，評估原則包括建構區域聯防體系、導入政府組態基準、完善資安基礎環境、提升資安自主產品使用，權重值，詳如下表：

項次	內容	占分比(%)
106-107年度執行成效	1.106年度經費執行率 2.106年-107年實際執行狀況(截至107年5月)	20
108-109年度推動重點	建構區域聯防體系	30
	導入政府組態基準	15
	完善資安基礎環境	20
	提升資安自主產品使用	15

為推動我國資通安全防護計畫，規劃各機關整體資通安全策略、審議資通安全計畫與資源分配，並推動政府整體資通安全規劃、建置及防護相關計畫，本院訂頒「行政院補助地方政府強化資通安全防護作業要點」，以補助地方政府資安防護相關計畫。

另依「中央對直轄市及縣市政府補助辦法」第 8 條規定，中央對直轄市及縣（市）政府之計畫型補助款，應依財力級次給予不同補助比率，除臺北市政府列為第一級外，其餘直轄市及縣（市）政府應依最近三年度決算審定數之自有財源比率之平均值為其財力，並依序平均分列級次如下：

一、直轄市政府列為第二級至第三級。

二、縣（市）政府列為第三級至第五級。

柒、 其他補充資料

附件 1：內政部

附件 2：財政部

附件 3：臺北市

附件 4：新北市

附件 5：桃園市

附件 6：臺中市

附件 7：臺南市

附件 8：高雄市

捌、106 年前瞻基礎建設計畫執行情形(截至 106/12/31)

一、進度及預算執行情形

主提機關 (含單位)	申請機關 (含單位)	法定數 (千元)	執行數 (千元)	保留數 (千元)
本院資安處	本院資安處	60,000	0	60,000
財政部	本院資安處	40,000	11,954	28,046
內政部	本院資安處	0	-	-

二、重要執行成果及目標達成情形

(一) 本院資通安全處

1. 本院於 106 年 9 月 21 日，訂頒「行政院補助地方政府強化資通安全防護作業要點」，並分行各地方政府配合辦理。

2. 本院於 106 年 12 月 19 日核定六都直轄市政府協同鄰近縣市政府提報之第 1 期(106 年度至 107 年度)前瞻基礎建設計畫經費。

(二) 財政部

1. 財政部於 106 年 9 月 25 日，訂頒「財政部補助地方稅稽徵機關強化資通安全防護作業要點」，並依規定於 106 年 11 月 10 日函送本院備查。
2. 106 年 10 至 12 月審查各地方稅稽徵機關提報之「強化政府基層機關資安防護及區域聯防計畫」。

(三) 內政部

1. 戶政司及地政司分別於 106 年 8 月 17 日、10 月 24 日完成 107 年度補助地方政府汰換戶役地政資訊設備盤點。
2. 戶政司於 106 年 10 月 31 日訂定「內政部補助地方政府強化戶役政基層機關資安防護及區域聯防計畫作業要點」，後續將依規定函送本院備查。

三、重大落後計畫之預警、輔導及管理

本院資通安全處將依據國發會訂定之「前瞻基礎建設計畫績效管考作業準則」執行計畫管考，管考方式如下：

(一) 每月掌握六都直轄市政府、財政部、內政部之計畫推動情形(含執行進度、預算支用、關鍵查核點達成情形、落後原因及因應對策等資料)，並依規定(每月 10 日前)上網(本院政府計畫管理資訊網(GPMnet))填報。

(二) 每季(4、7、10 月)召開計畫檢視會議，掌握六都直轄市政府、財政部、內政部之執行情形及遭遇困難。

(三) 視需要安排實地訪查，檢視各執行機關之資安防護設備採購進度、各地方政府整備網路架構進度、政府組態基準(GCB)政策及區域情資分享機制、建置等。

四、檢討與建議

配合特別預算於 106 年 8 月底審議通過，106 年 9 月 13 日總統公布施行後，本院資通安全處、財政部、內政部即刻展開補助地方政府說明會、計畫審查會議及訂頒中央補助地方政府作業要點等，惟各地方政府之 106 年度經費支用程序，依規定須檢具該地方政府配合款編列證明、地方議會同意墊付公文及採購招標契約等作業，始得申請特別預算補助款，又地方議會開議時程大多於 107 年 2 至 3 月召開，故本院將 106 年 12 月經費申請保留至 107 年 4 月執行。

另財政部主責本分項計畫，106 年 12 月編列 4,000 萬元，已執行 1,115 萬元，該部地方稅稽徵機關提出補助申請，同本院須檢具採購招標契約等相關資料，爰 106 年 12 月經費保留至 107 年 4 月，本院資通安全處業於 106 年 5 月 10 日邀集財政部與內政部召開計畫說明會，並訂每月追蹤地方政府配合款編列情形及採購進度，最遲於 107 年 4 月完成，以確保各直轄市及縣市議會開議時，取得同意墊付公文，俾利計畫如期如質執行。

附件 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之分項計畫

內政部

108 年 1 月

內政部(戶役地政)之基層資訊設備汰換整體計畫

一、計畫緣起

(一) 因應國際發展趨勢，政府刻正推動「服務型智慧政府推動計畫」，以「服務智慧政府」為願景，優先以民眾關切議題推動數位服務，契合民眾的需要，並提升國家數位競爭力，而本部戶役地政基層機關正是扮演「服務智慧政府」的重要推手；另依據數位國家創新經濟推動(DIGI+)主軸一【寬頻建設暨網路安全】推動資安基礎建設，提供網路安心服務，係以提升全國資訊與資安環境，保障國家及人民安全為目標。爰本部推動戶役地政各項創新服務時，為提供民眾需要及契合政府施政願景與目標，強化直轄市、縣（市）政府及基層機關資訊安全防禦能力正是當前重要課題。

(二) 本部於「前瞻基礎建設計畫」之「建構公教體系綠能雲端資料中心」中，提出「內政部資料中心整體建置計畫」，規劃以本部為中心設置綠能雲端資料中心，透過集中共享方式及資訊系統逐步整合；另於國家發展委員會「服務型智慧政府推動計畫」中，提出「內政跨域整合服務計畫(108-109)」藉以規劃創新內政數位服務，建構一站式服務與共用平台，以服務智慧政府為願景、契合民眾的需要，最終以達成一站式內政數位創新便民服務之目標。

爰此，本部戶政司提出「戶役政綠色便民及資安強化計畫」，配合上述計畫期程，規劃將現有戶政相關資訊系統移轉為雲端架構，納入本部雲端資源池環境，以提升主機資源使用率，達成本部及所屬資源共享與有效利用，共用資安防禦機制，並藉此推動創新戶政服務，提升簡政便民效益，打造戶政數位服務網，一改本部自民國 86 年 9 月全國連線作業之戶役政資訊系統架構。

(三) 依行政院資通安全辦公室 104 年度對本部（地政司）之資通安全稽核

報告，建議強化直轄市、縣（市）政府及各地政事務所之資安管理及資安健檢，充分掌握系統末端之資安情況。基層地政機關囿於地方財政困難，投入資通安全相關之經費不足，長年以來資訊軟硬設備難以更新，成為整體資安防護之潛藏風險；另為提供跨域登記服務，讓民眾可以在全國任一登記機關申辦土地登記案件，以提升為民服務品質，本部（地政司）刻推動跨縣市收辦土地登記案件，並配合行政院電子化政府政策，研提「開放地政跨域服務整合計畫」納入「服務型智慧政府推動計畫」子項計畫。

(四) 綜上，為配合上開計畫，地方機關辦理各項行政業務時，須取得本部重要基礎資料，爰本部資訊系統集中與強化其資安同時，有必要強化直轄市、縣（市）政府資訊安全防禦能力，現階段全國戶役政資訊系統，其軟硬體設備係於 99 年所購置，軟體或韌體版本老舊，存在著被攻擊的弱點無法修補，對於整體資安防護潛藏極大風險，而全國地政相關軟硬體設備亦面臨相同問題，配合本部推動跨縣市收辦土地登記案件，資安的防護更是刻不容緩，爰提報本計畫針對全國戶政、役政與地政進行老舊設備之汰換，強化資安防護設備及導入資安防護政府組態基準(GCB)，以降低基層機關遭入侵之資安風險及全面鞏固本部資訊安全防禦措施，保護本部關鍵基礎設施，朝向服務型智慧政府的願景邁進。

二、計畫目標

(一)辦理地方政府工作站及周邊設備更新，提升戶役政資訊系統及地政整合系統地籍資料庫關鍵基礎設施。

(二)辦理地方政府網路及資安設備更新，提升整體資安防護機制。

(三)導入基層機關政府組態基準規範，有效控制電腦遭受駭客入侵，以降低資安事件。

三、計畫內容與實施策略

為提供便民及親民服務之施政目標，達到強化政府基層機關資安防護與區域聯防之目標，並確保基層工作站及網路安全，本計畫預期達成目標之功作項目及內容分列如下：

(一) 汰換縣市工作站及便民服務設備，提升戶役政資訊系統與地政資訊系統之關鍵基礎設施：現行全國戶役政資訊系統之端末工作站、便民服務工作站等設備係於 99 年底購置，於 105 年底屆滿 6 年使用年限，故障率逐年提高，若未進行汰換，恐影響戶役政資訊系統正常運行。而地政資訊系統之端末工作站大多為 7 年前所購置，已逾使用年限，部分電腦設備甚至仍使用微軟 XP 作業系統，且 Windows7 作業系統亦將於 2020 年停止服務而無法更新，對於資安整體防護將衍生潛藏風險。故透過本計畫汰換基層老舊電腦設備及強化資安防護，提升便民服務效能。

(二) 汰換縣市網路及資安設備，降低機關用戶端及遭入侵之風險：戶役政資訊系統管理全國民眾戶籍、兵籍之隱私資料，地政資訊系統管理全國地籍資料，皆為政府機關資訊處理之基礎來源，需仰賴資訊安全設備來建構整體運作環境的安全，以戶政基層機關為例，路由器及交換器等網路及資安設備設備，於 99 年底購置後，因設備較舊，亦無法持續相關軟體、韌體升級或支援服務，存在著被攻擊的弱點無法修補，對於整體資安防護產生潛藏風險其資料之機密性、可用性及完整性影響民眾權益甚鉅；而基層地政機關現行網路設備大多為 100Mbps 的網路環境架構，資訊安全設備皆已購置 5 年以上，且防護架構多為不足，由於非法資訊攻擊行為之技術以及方式日新月異，資訊安全設備須經常保持最新的防護資訊及狀態，故需汰換及強化，才能提供安全的作業環境。

(三) 導入資安管制軟體及控管機制：

1. 戶役政機關將導入 AD(帳號認證管理)、GCB(電腦安全組態管理)及(NAC 網路存取控制控管)等機制，簡化管理之複雜度：將縣市工作站統及網路系統設備，透過 AD、GCB 及 NAC 網路存取控制控管機制集中化管理及監測，簡化管理之複雜度，提升基層機關資安防護，降低資安風險。

2. 由於地政資訊未來將導入集中化架構，各直轄市、縣(市)資料中心(Data Center)將負責該縣市地政資訊整合服務作業，資訊架構的各項訊息收集、分析以及管理機制的建置對於整體系統維運及安全管理相當重要。下列為本計畫強化資訊系統管理架構的項目及說明：

(1) LOG 分析管理平台：配合 ISMS 作業規範建立伺服器及資安網路。

(2) 遠端連線管控稽核平台：建構遠端連線管理及稽核平台(側錄)。

(3) GCB 稽核管理平台：配合政府組態基準 GCB 導入管理稽核。

(4) 資料庫稽核：提供資料庫存取安全防護稽核。

四、實施範圍

全國各直轄市、縣(市)政府及所轄戶役地政機關。

五、計畫期程：民國 108 年 1 月-109 年 12 月

六、關鍵績效指標及年度目標值

項次	關鍵績效指標	年度目標值
1	基層戶役政機關工作站便民服務設備建置率	108 年完成建置率達 95%以上。(累計新增設備建置數/總設備建置數*100%)。
2	汰換基層戶役地政機關網路及資安設備建置率	戶役政機關： 108 年建置率達 50%以上；109 年建置率達 95%以上(累計新增設備建置數/總設備建置數*100%)。 地政機關：108 年建置率達 50%以上；109 年達 95%以上(累計新增設備建置數/總設備建置數*100%)。
3	導入資安管制軟體及控管機制	戶役政機關： 108 年建置率達 50%以上，109 年達 95%以上(累計新增設備數/總建

		置數*100%)。 地政機關： 108 年建置率需達 50%以上;109 年達 95%以上(累計新增設備數/總建置數)。

七、持續營運評估

(一) 民眾服務面：戶役地政系統管理全國關鍵基礎資料，與提供民眾日常生活所需之政府服務息息相關，在提升民眾便捷服務時，加強系統資訊安全，提升系統中個人資料安全防護，更是戶役地系統重要考量。透過本計畫汰換縣市老舊工作站及多項便民服務設備等關鍵基礎建設，提升行政效率，縮短民眾等候時間，滿足民眾對公部門服務之期許，達到簡政便民之目標，同時本計畫於完成後，透過統一資安縱深防禦機制，更強化基層機關資安防護及區域聯防，確保基層戶役地機關資訊作業之持續性，避免因不可預期的事件影響業務，使戶役地政作業單位得以延續原已廣獲全國民眾好評之高品質服務，並不斷配合時代潮流及技術發展，提供更安全、創新、便民之服務措施，達到營運不中斷，以支援政府再造，邁向全民智慧型政府。

(二) 機關資安面：隨著科技的演進，資安威脅日趨嚴重下，秉持資安亦國安的原則，本計畫在汰換基層機關超過使用年限或停產之資訊軟硬體設備，包括伺服主機及資安防護設備，提升建構戶役地基層機關資安防護，降低系統因老舊無法更新而導致資安漏洞、駭客入侵之風險，同時導入資安管制軟體及控管機制，將縣市工作站統及網路系統設備，透過 AD、GCB 及 NAC 網路存取控制控管機制集中化管理及監測，強化資安端點防護，並簡化管理之複雜度，以確保各項重要基礎資料能安全無虞共用共享，透過統一資安縱深防禦機制，更強化架構基層機關資安防護及區域聯防，以達到持續經營的效用。

(三) 廠商營運面：依據前述規劃之實施範圍及工作項目，本計畫在採購資通訊安全設備時，將以國產品為優先採購標的，連結在地能量及扶持本土資安廠商理念，著重在地服務及過去實績，優先採用本土優良廠商協商

將國內資安產品納入政府同共供應契約，提高資安軟硬體國產品採購比例，帶動國內資安產業之蓬勃發展。

八、經費明細概算

(一)本計畫汰換基層戶役政電腦相關設備計分 8 項目，總經費需求約為新臺幣(以下同)1 億元，詳附基層機關(戶役政)經費預估表。

1.汰換縣市工作站及周邊設備

各縣市便民服務工作站及其他周邊(780 套)，總計約 3,822 萬元。

2.汰換縣市網路及資安設備

(1)新世代防火牆系統(22 部)、通訊主機(22 部)，設備計 44 部，總計經費約 3,520 萬元。

(2)防毒/防駭系統(780 台) ，總計經費約 312 萬元。

3.導入 AD、GCB、NAC、終端資安管制軟體及控管機制

導入 NAC(805 台)、GCB(780 台)、AD(780 台)及終端資安管制軟體(9,865 台)，總計經費約 2,346 萬元。

單位：新臺幣(千元)

年度	項次	工作項目	工作內容	所需經費		績效目標	**優先次序(必填)**
				經常門	資本門		
108	1	汰換工作站	汰換便民服務工作站及防毒/防駭系統等		41,340	建置率達95%以上	1
	2	汰換網路及資安設備				建置率達50%以上	1
	3	導入資安管制軟體及控管機制	增加 NAC 網路存取控制)、GCB(電腦安全組態、AD(帳號認證管理)等。		8,660	建置率達50%以上	2
109	1	汰換網路及資安設備	汰換新世代防火牆系統及增加通訊主機等。		33,200	建置率達95%以上	1
	2	導入資安管制軟體	增加終端資安管制軟體		14,800	建置率達95%以上	2

		及控管機制	等。				
合計				98,000			

(二)本計畫汰換基層地政機關電腦相關設備項目計 14 項，108 年及 109 年總經費需求 1 億元，詳附基層機關(地政)所需經費預估表：

1.汰換直轄市、縣(市)政府地政局（處）及所轄地政事務所端網路及資安設備，包括：地政資料中心用防火牆(含 IDP 入侵偵測防護系統)(1 套)、地政事務所防火牆(9 套)、資料中心用高速儲存設備(1 套)、資料儲存平台(3 套)、連接終端設備之群組交換器(18 部)、伺服器或虛擬化架構(5 套)。合計 2,130 萬元。

2.導入資安管制軟體及控管機制

導入 LOG 分析管理平台(22 套)、遠端連線管控稽核平台(15 套)、GCB 稽核管理平台(16 套)、資料庫稽核(14 套)。合計 7,870 萬元。

單位：新臺幣(千元)

年度	項次	工作項目	工作內容	所需經費		績效目標	**優先次序(必填)**
				經常門	資本門		
108	1	汰換網路及資安設備	直轄市及彰化縣、嘉義縣等 8 市縣汰換防火牆、資料儲存平台、群組交換器、伺服器或虛擬化架構等設備。		11,800	建置率達50%以上	1
	2	導入資安管制軟體及控管機制	直轄市及彰化縣、嘉義縣等 8 市縣導入 LOG 分析管理平台、遠端連線管控稽核平台、GCB 稽核管		38,200	建置率達50%以上	2

			理平台、資料庫稽核等軟體。				
109	1	汰換網路及資安設備	宜蘭縣等 14 縣(市) 汰換防火牆、速儲存設備、資料儲存平台、伺服器或虛擬化架構等設備。		9,500	建置率達95%以上	1
	2	導入資安管制軟體及控管機制	宜蘭縣等 14 縣(市) 導入 LOG 分析管理平台、遠端連線管控稽核平台、GCB 稽核管理平台、資料庫稽核等軟體。		38,500	建置數達95%以上	2
合計				98,000			

九、預定進度

時程	累計預定進度(%)	累計預定支用費用(千元)	關鍵查核點
108	50%	100,000	戶役政機關： 108年12月底前汰換全國戶役政機關老舊PC及導入GCB等資安管制軟體及控管機制。 地政機關： 108年12月底汰換直轄市及彰化縣、嘉義縣等8市縣網路及資安設備，並導入資安管制軟體及控管機制。
109	100%	196,000	戶役政機關： 109 年 12 月底前汰換全國戶役政機關老舊主機及導入資安控管機制。 地政機關： 109 年 12 月底汰換宜蘭縣等 14 縣(市)網路及資安設備，並導入資安管制軟體及控管機制。

十、預期效益

(一)本計畫之順利推動，將使基層機關戶役地政作業單位得以延續原已廣獲全國民眾好評之高品質服務，並不斷配合時代潮流及技術發展，提供更創新、便民之服務措施，讓電子化政府更值得民眾信賴。

(二)本計畫充分運用資訊新科技，一方面提高行政效能，創新政府的服務，一方面提升便民服務品質，支援政府再造，邁向全民智慧型政府。

(三)本計畫於完成後，透過統一資安縱深防禦機制，更強化基層機關資安防護及區域聯防。

(四)本計畫於完成後，對內部工作站使用網路資源存取控制管理，及外部的網路連接控制管理，可大幅增加管理的效率。

十一、相關聯絡資料

單位	聯絡人姓名	職稱	電話	E-mail
內政部資訊中心	王瓊苑	科長	02-25132222	Moi1025@moi.gov.tw
	賴金蘭	技正	02-25132226	Moi0565@moi.gov.tw
內政部戶政司	黃旭初	科長	02-89127501	Moi0499@moi.gov.tw
	王宗隆	約聘研究員	02-89127528	Moi5660@moi.gov.tw
內政部地政司	陳永志	科長	04-22544496#200	czester@land.gov.tw
	洪欽雄	視察	04-22511196#202	hct@land.gov.tw

內政部(警政署)建置電腦端點資安聯防及人才培育計畫

一、計畫緣起

為因應目前科技進步快速、駭客攻擊手法多變之挑戰，並遵循國家科學技術發展之目標與願景，以及資通安全管理法規範資安專責人才之要求，規劃持續執行「建置電腦端點資安聯防及人才培育計畫」，藉此提升警察機關資安防護軟、硬體能量，並培育相關資安科技人才，戮力達成總統指示「資安即國安」之重點工作，俾利提升警政機關的資通訊安全防護能量。

二、計畫目標

網路駭客犯罪手法日益變化並使用複雜的科技技術，較傳統防護模式更具技術難度，大規模的資安事件常引發民眾恐慌，影響不容小覷。總統於 106 年 1 月 6 日出席本部警政署務會報時，提出兩項治安重點工作，「需特別留意網路犯罪問題，提高追查力道」及「國家要走向數位經濟的時代，維持公正和安全的網路環境，是必要的基礎工作」，顯現資訊網路安全之重要性。

自 105 年起，國內陸續發生大規模的資安事件，105 年國內發生首宗提款機遭盜領案「第一銀行 ATM 盜領案」、106 年 2 月起陸續發生大規模券商及學校遭恐嚇 DDoS 攻擊並威脅支付比特幣案件，以及 106 年 10 月發生國際矚目「遠東銀行案遭駭侵案」等事件，顯見當前駭客攻擊威脅及危害層面廣泛，且犯罪者隱身於網路環境追查不易，突顯我國正面臨科技能量重大挑戰，提升資訊安全科技能力已勢在必行。面對國內近年駭侵事件範圍擴大、受害程度愈趨嚴重，如何儘快掌握國內、外駭客集團動向，或於資安案件中找出可疑惡意程式跡證，保全數位證據，以利後續控管、減少損害。

為強化政府整體資安防護作為，持續建置本部警政署與所屬重點機關之電腦端點資安防禦能量，以提升本部警政署資安防護能力與針對駭客入侵、阻斷服務及網路勒索之網路跡證資安事件分析效能，並透過警政資安

事件分析中心資安聯防建置，提供警政執法機關資安防護狀況感知、快速行動反應以及情報驅動聯防之國家建置層級資安防護分析與情報分享平臺，藉由行政院資通安全處之資安聯防與情資分享架構，以進行警政資安情報與網路資安事件情報分享，提供病毒碼特徵、端點行為、中繼網址、連線數位跡證資料，作到早期預警、持續監控、通報應變與協處改善之資安整備與聯防，並訓練資安專業人才，提升資安自主能量。

三、計畫內容與實施策略

建置電腦端點資安聯防及人才培育計畫

1.計畫架構：

本計畫目標擬建置本部警政署與所屬重點警察機關之電腦端點資安防禦能量，以強化警政機關資安防護能力與針對駭客入侵及惡意程式感染等各種攻擊之跡證事件蒐集效能，並透過警政資安事件分析中心及資安聯防建置，提供警政執法機關資安防護狀況感知、快速行動反應以及情報驅動聯防之國家建置層級資安防護分析與情報分享平臺，由「警政資安團隊」分析並提供病毒碼特徵、端點行為、中繼網址、連線數位跡證資料，達到早期預警、持續監控、通報應變與協處改善之資安整備與聯防，並藉由行政院資通安全處之資安聯防與情資分享架構，以進行警政資安情報與網路資安事件情報分享，以強化政府整體資安防護作為。另亦訓練「警政資安團隊」成員資安健診、設透測試及弱點檢測等能力，以增進資安技術自主能量，並透過個人資料安全管理系統，強化個人資料保護能力。

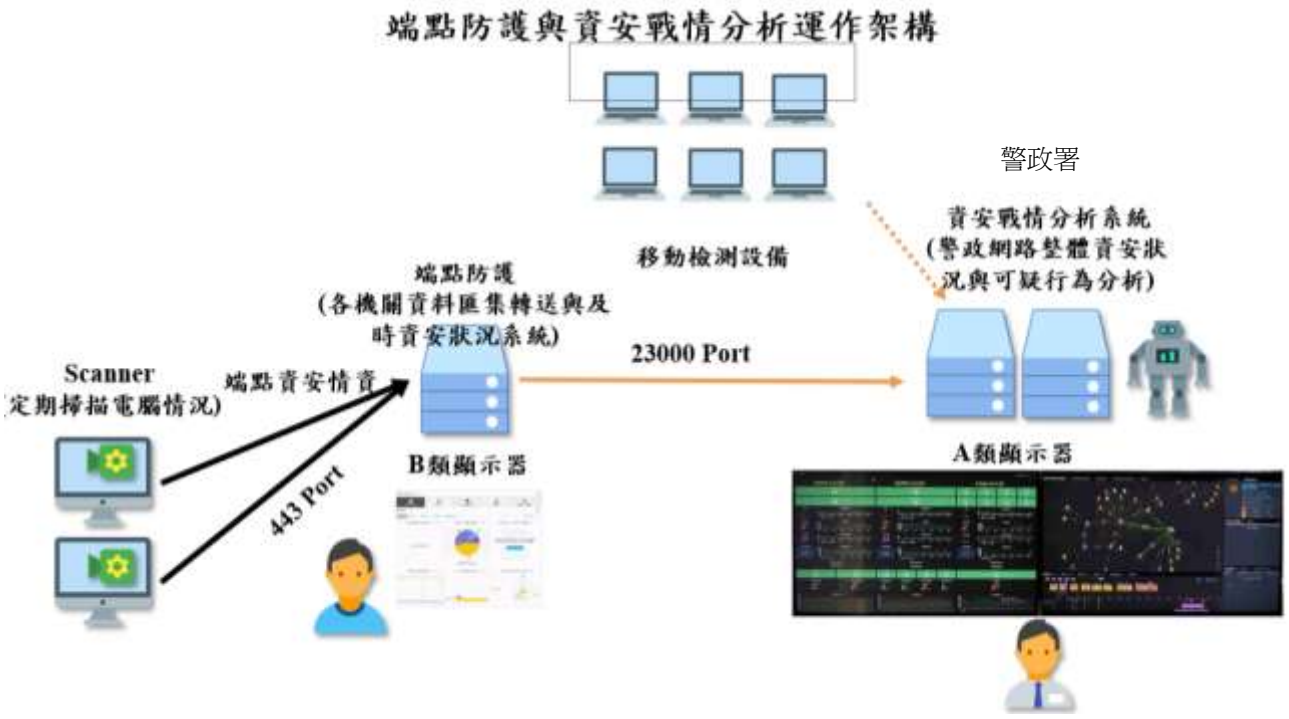
2.計畫說明：

為因應資通安全管理法對資安之重視，規劃警政機關資安防護與網路資安事件之端點資安防護需求，進行配賦與導入作業，108 年度持續導入本部警政署所屬機關警察局端點防護工作。

3.工作項目：

(1)端點資安防護分析工具

提供員警針對網路資安事件與執行本署所屬機關資安防護用戶端所需之端點資安防護分析工具，藉由端點行為分析與端點防護之端點偵測回應(EDR)技術，並結合國家級資安聯防分享情資，達到早期或定期之警政執法機關資安事件狀況感知、快速行動反應與強化資安威脅能見度之資安要求，本資安防護工具配賦原則，擬依勤務優先順序以三年期間分期進行配賦，配賦範圍將涵蓋全國警政機關，108 年度規劃建置本部警政署所屬刑事警察局、航空警察局、國道公路警察局及鐵路警察局等 4 機關，配賦規劃詳述如下表。



(2)資安防護及情資諮詢服務

為強化員警端點資安防護工具部署，深化資安分析技術，除了藉由委外/徵集方式，引進種子教官或資安顧問，透過資安防護諮詢/案例協處方式進行作業，以擴大應用層面並落實執行成效，長期則

藉由資安訓練定期課程或資安研討會等方法推動，並經由培訓/徵集本署相關網路資安全認證人員，持續訓練與擴大警政資安專家團隊，專責進行警政機關資安防護與資安事件防治技術推動與管理，並培訓警政機關資安健診、滲透測試、弱點檢測之人才，提升資安自主能量。

(3)資安事件綜合分析顧問服務

依行政院「資通安全通報應變作業機制」、「行政院及所屬各機關資訊安全管理要點」、「行政院及所屬各機關資訊安全管理規範」，提供本署及所屬機關之警政資安防護及分析中心資安事件綜合分析顧問服務與協助執行資安應變計畫，其內容敘述如下：

1. 資安防護分析：分析災害影響範圍與程度，判定資安事件影響等級。
2. 資安事件緊急應變措施：經判定資安事件立即通報、執行復原或損管作業、結案通報。
3. 即時分享警政資安與網路犯罪偵防資安情報，交換病毒碼特徵、端點行為、中繼網址、連線數位跡證情資，依安全通報分享情報，進行早期資安事件分析與緊急應變措施，強化落實政府整體資安聯防效能。

短期將透過委外專業資安顧問之資安事件分析協助與案例諮詢方式，以最短時間獲致最大成效，長期則規畫交由警政資安專家團隊，專責進行警政機關資安防護與資安事件防治技術推動與管理。

四、實施範圍

實施對象：內政部警政署、刑事警察局、航空警察局、國道公路警察局、鐵路警察局

五、計畫期程

108 年 1 月 1 日至 108 年 12 月 31 日止。

六、關鍵績效指標

(一) 持續建置本部警政署所屬機關端點防護平臺，共計 4 個單位。

(二) 產出資安情資分享及交流計 12 次。

(三) 警政資安團隊實施資安健診、滲透測試、弱點檢測共計 6 次。

七、持續營運評估

「建置國家資安機制，提升自我防護能量」為國家重要政策，「建置電腦端點資安聯防及人才培育計畫」以警政機關之整體資安防護、培育資安技術人才為主要目標，提升資通安全、防止重大資安事件發生及機敏性資料外流，因此應永續經營，除以既有之公務預算支應外，將積極爭取其他預算以利持續營運。

八、經費明細概算(建議參考計畫期程中的表格內容)

(一)本年度(108 年 1 月 1 日至 108 年 12 月 31 日)本計畫經費預估投入 8,000 千元，分配情形，詳如下表

經費項目		經費(千元)	用途
經常門	1. 用戶端點資安防護工具 2. 資安防護及情資諮詢服務、資安事件綜合分析顧問服務、培育專業資安人才	6,960	1.建置 3,633 臺端末設備防護架構 5,450 千元。 2.導入資安防護及情資諮詢服務 860 千元 3.導入資安事件綜合分析顧問服務 650 千元
資本門	中階伺服器	1,040	於本部警政署所屬機關 4 個單位，配置端點防護資料伺服器
合計		8,000	

九、預定進度(建議參考計畫期程中的表格內)

108 年度預定進度

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
108 年 3 月	10%	0	完成招標及專案管理計畫書徵求
108 年 7 月	50%	0	持續建置系統、教育訓練及資安服務
108 年 10 月	100%	8,000,000	完成驗收及付款

十、預期效益

(一)蒐羅資安攻擊事件並導入專業情資及分析服務，導入 AI 智慧引擎透過區域性攻擊情資整合及視覺化關聯分析，發掘駭客攻擊戰術，釐清駭客組織之攻擊模式，並加以研擬防護偵測技術及因應對策。

(二)透過研析病毒碼特徵、中繼站資料、惡意程式碼、惡意軟體等各種重要之資安情資，與各警政相關機關、單位分享及交流，深化資安聯防機制，強化政府資安防護整體作為。

(三)培育警政機關資安技術專業人才，強化資安自主能量，協助全國警察機關實施資安健診、滲透測試、資安事件處理等各項資訊安全工作及稽核，並節省未來公帑支出。

十一、相關聯絡資料

單位	姓名	連絡電話	電子郵件
內政部警政署主任	蘇清偉	02-23931791#6040	frank@npa.gov.tw
內政部警政署科長	李崇偉	02-23931791#6133	s601256@npa.gov.tw
內政部警政署技正	李權龍	02-23931791#6134	npa6015@npa.gov.tw
內政部警政署警務正	施能新	02-23931791#6155	sns@npa.gov.tw
內政部警政署技士	蕭澄航	02-23931791#6102	im751193@npa.gov.tw

附件 2

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之分項計畫

財政部

108 年 1 月

一、政策依據

(一) 行政院「前瞻基礎建設計畫」

摘錄該計畫「數位建設」建設主軸 4.1.2「強化政府基層機關資安防護及區域聯防」計畫概要如下：

政府機關經費有限，長久以來資訊設備難以如期汰換更新，致部分個人電腦或伺服器作業系統無原廠維護或無法配合更新軟體版本，造成整體資安防護潛藏風險。

本計畫重點將以汰換超過年限（高風險）之資訊設備為主，範圍包括戶政、役政、地政、稅務及基層公所等，以降低基層機關用戶端及資訊系統遭入侵之風險。

(二) 行政院資通安全處「強化政府基層機關資安防護及區域聯防計畫」摘錄該計畫重點工作如下：

1. 汰換超過使用年限或停產之資訊軟硬體設備，範圍包括戶政、役政、地政、稅務、衛政、社政及基層公所等超過 7 年以上之 WindowsXP 個人電腦約 10 萬臺及資安防護設備等，強化政府資安端點防護，完備縱深防禦。

2. 軟硬體設備汰換以國產品為優先採購標的。

(三)「強化政府基層機關資安防護及區域聯防計畫第三次研商會議」決議摘錄行政院資通安全處 106 年5 月10 日召開該次會議決議如下： 有關強化基層機關資安防護能量，汰換超過年限（7 年以上）之資訊設備（伺服主機、個人電腦），其中戶政、役政、地政、稅務由內政部及財政部統籌規劃執行。

二、擬解決問題之釐清

依行政院「財物標準分類」，主機系統最低使用年限為 5 年，個人電腦為 4 年。經初步調查，財政部暨其所屬機關及各直轄市、縣

（市）政府（以下簡稱各地方政府）所屬地方稅稽徵機關於 100 年以前所購置之個人電腦逾 2 萬部、伺服主機逾 2,000 部，至 107 年，該等設備使用已逾7 年，急待汰換、擴充或更新。

106 年初爆發之 WannaCrypt 勒索軟體威脅，主要係個人電腦及伺服主機之作業系統未及時安裝修補程式（patch）所致。如相關設備作業系統及工具軟體逾停止支援（End of Support，以下簡稱 EOS）期限後，原廠將不再提供修補程式，此部分設備急需汰換、擴充或更新，以降低資安威脅。茲列舉部分 EOS 期限如下：

作業系統或工具軟體	EOS
IBM HTTP Server 7	107 年
IBM WebSphere Application	107 年
SQL Server 2008 R2	108 年
Windows 7	109 年
Windows Server 2008 R2	109 年
Exchange 2010	109 年

三、計畫目標

目標說明

(一) 全面強化基層機關資安防護，完備國家資安基礎建設。

(二) 強化財政資訊共用系統防護，提供安全資訊作業環境。

(三) 提升國內資通訊自主產品。

執行策略及方法

本計畫由「基層機關」及「財政資訊業務主管機關」分別進行端末設備及主機系統之資訊安全強化，並分述如下：

(一) 全面強化基層機關資安防護

1. 基層機關，包含：

(1) 財政部所屬機關，但不含國庫署本署、關務署本署、國有財產署本署及財政資訊中心。

(2) 地方政府所屬地方稅稽徵機關。

2. 工作內容

(1) 汰換（含擴充或更新）基層機關超過使用年限或停產之資訊軟硬體設備，範圍包括於本計畫期程內使用超過 7 年以上之個人電腦、伺服主機及資安防護設備等。

(2) 強化政府機關之資安端點防護，完備縱深防禦。包含：防毒軟體、資產管理軟體、登入管理（如：AD 網域）及資安防護與鑑識軟硬體等。

(3) 基層機關配合導入政府組態基準（Government Configuration Baseline，簡稱 GCB），以規範資通訊終端設備（如：個人電腦）的一致性安全設定（如：密碼長度、更新期限等），降低駭客入侵引發資安事件之風險。

3. 補助作業

各地方政府所屬地方稅稽徵機關之補助作業，依照「中央對直轄市及縣（市）政府補助辦法」，並比照「行政院資通安全處補助地方政府作業要點」（註：現行為草案）辦理，由受補助機關提出申請，財政部財政資訊中心辦理審核、撥付及考核等相關事宜。

(二) 強化財政資訊共用系統防護

1. 財政資訊業務主管機關，包含：

財政部本部及所屬國庫署本署、關務署本署、國有財產署本署及財政資訊中心。

2. 工作內容

(1) 辦理汰換（含擴充或更新）超過使用年限或停產之資訊軟硬體設備、強化政府機關之資安端點防護及導入政府組態基準等。

(2) 財政部國庫署、關務署、國有財產署及財政資訊中心分別統籌辦理國庫、關務、國產及賦稅（含國稅及地方稅）等共用資訊系統及軟硬體平臺。以賦稅資訊系統為例，整合各地區國稅局及各地方稅稽徵機關之國稅及地方稅資訊業務，其資安防護為前列基層機關之資安核心需求，且共同聯防具經濟效益。為提供安全資訊作業環境，財政資訊業務主管機關就各主管之共用資訊系統及軟硬體平臺辦理下列事宜：

a. 就整體資訊作業環境評估共用資訊系統及軟硬體平臺之優先汰換（含擴充或更新）序列。

b. 汰換（含擴充或更新）序列以外網系統優先、為民服務系統優先、核心業務系統優先。

c. 汰換（含擴充或更新）範圍包含所需之個人電腦、伺服主機、網路設備、資安防護設備、作業系統及工具軟體等。

(三) 提升國內資通訊自主產品使用

資通訊軟硬體設備汰換以國產品為優先採購標的，全案 50%經費採購國產品為目標。

四、預期效益

(一) 藉由汰換(含擴充或更新)基層機關超過使用年限或停產之資訊軟硬體設備，強化政府機關之資安端點防護，完備縱深防禦，降低基層機關遭入侵之資安風險，提升政府整體資安防護水準。

(二) 強化國庫、關務、國產及賦稅(含國稅及地方稅)等共用資訊系統及軟硬體平臺，提供政府機關安全資訊作業環境。

(三) 資通訊軟硬體設備汰換以國產品為優先採購標的，全案 50%經費採購國產品為目標，藉以帶動國內資通訊產業之發展。

五、績效指標

年　度	106	107	108	109
績效指標	量化指標(%)			
1. 汰換（或擴充及更新）基層機關 7 年以上電腦主機及資安防護設備。	5	50	80	90
2. 基層機關導入政府組態基準。	10	60	80	95
3. 提升國內資通訊產品使用率。	0	10	25	50

附件 3

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之分項計畫

臺北市

108 年 3 月

臺北市暨花蓮縣、金門縣及連江縣政府
區域聯防計畫

一、計畫緣起

近年全球網路安全(Cyber Security)威脅事件不斷提升，美國FBI所屬IC3公布2016年網路犯罪損失金額達400億台幣、各國關鍵基礎設施及醫療機構亦傳出遭駭客滲透或遭勒贖病毒入侵等情事，且隨著物聯網（Internet of Things, IOT）日趨普及，網路安全已成為各國必須嚴肅面對的課題。

現行中央及地方政府雖已依「政府機關（構）資通安全責任等級分級作業規定」進行資通安全責任等級分級，並依機關資安責任等級之應辦事項辦理相關作業，如不定期辦理社交工程演練、網路攻防演練、核心系統須通過ISMS第三方認證、資安防護縱深要求、委外建置資訊安全運作中心（Security Operation Center, SOC）等，然隨著網路犯罪組織化及專業化、攻擊成本降低，相較於攻擊只需針對單一弱點即可入侵成功，組織已難以避免不被入侵，相對的應建立持續性的監控及即時回應機制，縮短遭入侵所受到的損害，而地方政府面對資安的挑戰也更具艱難，主要問題分述如下：

(一) 地方政府資安人力缺乏且制度及管理面上難以訂定適合之資安防護政策及落實資安防護要求：目前中央與地方資安人力缺口至少一千人以上，且各機關資安人力甚至多為「兼任」而非專職。在此條件下，地方政府雖可依中央訂定之相關法規辦理，然在政策制訂、系統建置、資安服務採購上皆缺乏可實際落實之共通性要求及經驗。

(二) 資安經費長期偏低：本府資訊安全佔資通訊預算比104至107年皆低於5%，遠低於中央各部會，可見資訊業務擴張同時，資安防護卻未能跟上。

(三) 技術過度倚賴廠商：政府機關資訊業務大量委外，而涉及到政府系統及資料安全的業務亦屬委外之一部份，造成資安核心技能無法掌握，導致監控品質不佳及處理資安業務時效無法即時。

(四) 缺乏資通安全共享情資機制：現行除行政院國家資通安全會報技術服務中心不定期提供資安警訊外，各地方政府所建立(或委外)SOC，亦處理資安事件及發現惡意程式樣本，然而各地方政府僅針對所維護之單位連線行為進行分析及處理，缺乏跨地方政府之綜合分析。故如單一地方政府發生攻擊事件，相關情資(如攻擊手法、中繼站、惡意程式樣本) ，無法立即告警其餘地方政府。

(五) 資安事件緊急應變能量不足：網路攻擊手法層出不窮，現行政府機關對於通報之流程面已具備一定程度之熟稔，然對於緊急之資安事件尚無法即時掌握攻擊方式及影響範圍，往往對於不明確之通報僅能刪除惡意程式或重灌電腦以確保安全，反而遺失重要軌跡資料。

(六) 系統安全缺乏單一檢測機關及標準程序：資訊系統往往具大量個人資料或機敏資料，且對外系統往往成為駭客入侵的中繼站，並轉而入侵內部系統，取得更機敏之資料。然現行地方政府可依行政院訂定之「系統分級及資安防護基準」進行基本要求，更應於系統上線前及開發過程中訂定更嚴謹且可操作之系統檢測服務，讓機關得以將系統開發之心力回歸於系統面，安全面則由專責單位進行協助檢測。

(七) 電腦設備及資安防護設備老舊：政府運作已脫離不了使用資訊設備,各地方政府之資安預算往往偏低（詳下表），且現行隨著攻擊手法匹變，單一設備已經無法防護攻擊，必須透過縱深防護之概念，從閘道端、電子郵件防護、到用戶端、資料庫皆須佈屬相關設備。更甚者，部分機關甚至仍使用停止更

新支援之作業系統（如Windows Server 2003、Windows XP）致機關之系統存在高度風險。

(八) 資安廠商能力良莠不齊，資安人才缺乏：相較於以色列鼓勵創新，針對資安人才給予產業補助，現行台灣缺乏良好的資安環境，故此資安人才往往流向其他科技業及其他資訊業，造成資安界雪上加霜的困境，然而資安防護的好壞，與資安人員能力有絕對之關係，在此情況下造成資安產業能量不足，政府機關在大量委外情況下亦受到嚴重影響。

(九) 關鍵基礎設施防護薄弱：鑒於近年國際間關鍵基礎設施攻擊事件頻傳，除中央主管機關外，縣市政府亦掌管關鍵機處設施(如本府管理大眾捷運系統、北自來水等)，基於關鍵基礎設施之OT與傳統企業組織防護重點IT截然不同，前者重視穩定後者重視效率安全，致多年來其資安防護一直較疏於重視。

二、計畫目標

綜上，本計畫目標如下：

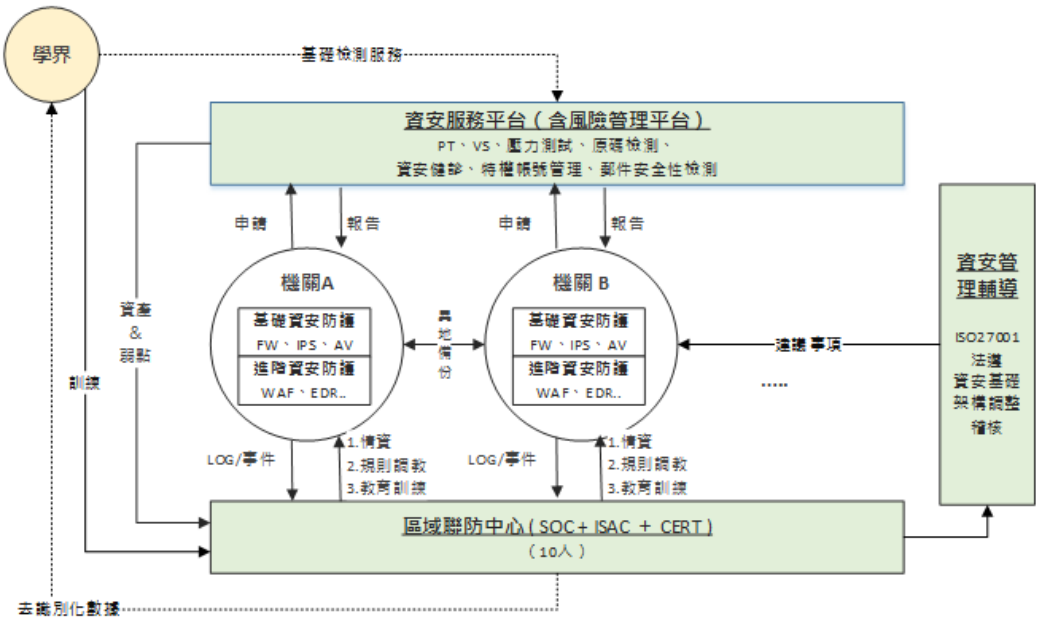
(一) 建置區域資安防護中心，透過整合臺北市政府、花蓮縣政府、金門縣政府、連江縣政府之 SOC、ISAC、CERT，以達到區域間情資互換、協同防護之綜效。

(二) 完善區域內各縣市資安管理制度，提升 GCB 導入比例並汰換 EOS 之主機，降低被入侵之機會。

(三) 提升機關資安人員能力及當地大學資安人才，增加資安整體產業能量，並建立產業合作模式，使業界及政府部門形成雙贏之模式。

三、計畫內容與實施策略

本計畫預計執行框架如下圖，包含「建置區域聯防中心」(SOC、ISAC 及 CERT）及「提供資安管理輔導制度」，並將相關資料提供予學界進行研究分析，各縣市政府並可互為資料異地備份中心，避免區域性災難造成資料遺失之問題，內容分述如下：x`



圖一、區域聯防暨強化資安基礎建設框架

(一) 強化基層機關資安防護，落實國家資訊基礎建設防護。

1. 落實資通安全責任等級要求

(1) 針對本府重要系統進行滲透測試及健檢服務(核心資訊系統及具大量個人資料、機敏資料之系統)，及早發現可能風險並強化機關現行所缺乏之資安防護設備。

(2) 預計執行對象及數量：依本府機關資安責任等級進行，至少 100 個系統。

(3) 預計執行時間：106~109 年。

2. 導入政府主態基準(Government Configuration Baseline, GCB)

(1) 藉由導入 GCB，強化作業系統組態安全，降低駭客入侵管道。

(2) 預計執行對象及數量：依本府各機關資安責任等級導入，逐年導入比例分別達 60%、80%、95%。

(3) 預計執行時間：107~109 年。

3. 建立弱點掃描管理平台(資產風險管理平台)。

(1) 針對本府各機關建制弱點掃描管理平台，已掌握各機關系統之弱點，使機關得以及時修補漏洞，主要功能包含：網頁及主機弱點掃描功能、依帳號權限管控主機弱掃功能、報表功能、弱點處理及修補建議功能、弱點複測功能。

(2) 預計執行對象及數量：本府伺服器區系統優先，視經費評估納入用戶端主機。

(3) 預計執行時間：107~109 年。

(二) 建立區域聯防機制，強化鄰近縣市資安防護能量

1. 深化縣市政府 SOC 內監控範圍、擴大區域內各縣市政府監控範圍：縣市政府內 SOC 監控範圍將收冗現行各自監控之機關，以利主管機關即時回應資安事件。
2. 建置及維運 ISAC 平台：透過蒐集國內外情資、交換及分析，獲得政府機關資安威脅及弱點，以儀表板方式呈現區域內資安狀況，並具有整體趨勢分析功能、自動化派送資安防護政策功能；另針對 ISAC 分析人員提供教育訓練、並利用學界合作，同時培育學界及政府處理資安事件經驗及能量，包含定義核心業務項目、識別情資範圍、確認分享對象、群組權限控管等項目。
3. 資安聯防設備增購及佈屬：機關除需達行政院所定對機關資通安全責任等級防護縱深之要求外，為能獲得更完整的監控資訊，應考量加入進階防護設備，如端點偵測及回應工具（Endpoint Detect and Response, EDR）、威脅入侵評估（Compromised Assessment Tool），並將其可用資訊傳遞至 SOC 以利事件進行綜合判別。
4. 預計執行對象及數量：現行自行建置或委外建置 SOC 之機關，並視經費增加資安設備深化監控範圍至 B 級或 C+級機關。
5. 預計執行時間：107~109 年。

(三) 成立跨縣市資安事件緊急處理小組

本府將於聯防中心內成立跨縣市資安事件緊急處理中心（Computer Emergency Response Team, CERT），建立區域應變團隊及資安事件應變流

程，掌握資安事件處理進度、落實並回饋資安事件處理機制。

協助鄰近縣市於發生重大資安事件時得以立刻支援確認受駭範圍、發生原因、入侵方式並協助回復系統正常運作，工作包含：建置戰情中心，導入端點偵測（或阻擋）機制、CERT 流程、建立通報及處理程序等、通報演練、定期追蹤資安事件等。

為能俾利後續與領域 SOC、ISAC 等進行資訊交流，系統宜採用 Structured Threat Information eXpression (STIX) 與 Trusted Automated eXchange of Indicator Information(TAXII)，以建置資安事件傳輸格式與傳輸架構。

(四) 結合區域大學能量合作

本計畫所列之相關建置維運（SOC、ISAC 及 CERT）、教育訓練及資安服務，呼應資安及國安之政策發展，將透過產官學合作模式，由學界提供前瞻性計研究、基礎資安檢測，由產業界提出資安新創需求，政府提供場域，以提升國家資安能量並持續培育本國資安人才。

四、實施範圍

本計畫實施對象為臺北市政府、花蓮縣政府、金門縣政府及連江縣政府。實施區域於 SOC、ISAC 及 CERT 包含前述政府機關，人才培育以各地方政府 A、B 級機關資安人員優先。系統汰換及資安檢測以核心系統或具大量、特種個資之系統。

五、計畫期程

項目	107	108	109
強化基層機關資安防護，落實國家資訊基礎建設防護	1. 本府 GCB 導入機關（A、B 級）比例達 60%。 2. A、B 級機關核心系統及具大量個資系統進行滲透測試。 3. 強化資安基礎防護：至少增加 DDOS 防護及導入解密設備。 4. 辦理紅隊演練。	1. 本府 GCB 導入機關（A、B 級）比例達 80%。 2. 針對本府重要系統進行滲透測試、弱點掃描及資安健檢。 3. 建立弱點掃描管理平台。	1. 持續檢視本府 GCB 導入情形，導入機關（A、B 級）比例達 95%。 2. 持續追蹤並針對本府重要系統進行滲透測試、弱點掃描及資安健檢。
建立區域聯防機制，強化鄰近縣市資安防護能量	1. 完成各縣市政府一線 SOC 建置及二線 SOC 收容。 2. 建立 CERT 機制。	1. 建置 ISAC。 2. 提供至少 2 件內部情資分享。 3. 完成每月二線 SOC 資安趨勢分析。	1. 持續提供 SOC、ISAC 及 CERT 服務。 2. 提供至少 4 件內部情資分享。
結合區域大學合作	培育政府資安人才（含技術及管理稽核）：至少取得 20 張國際資安認證。	規劃提供去識別化資料事件進行案例分析。	提供去識別化資料事件進行案例分析。

六、關鍵績效指標及年度目標值

詳第五點。

七、持續營運評估

本計畫將於 109 年評估後續區域聯防是否自維自運，若中心仍為委外（採購服務），以 10 人進行分析、通報及遠端事件處理作業（含產品 MA）、餘系統（CERT、ISAC）MA 費用（以 15%估算）及 SOC 約須每年約須 2,000 萬，就本府現行資安經常性預算約 6,500 萬，尚足以持續營運區域聯防中

心。後續並將持續依每年服務水準及設備狀態進行調整，並滾動式修正經費。

八、經費明細概算

單位：新臺幣

年度	項次	工作項目	工作內容	所需經費		績效目標	優先次序（必填）
				經常門	資本門		
臺北市政府							
107	1	區域聯防服務	1.建置二線 SOC、CERT，含內部情資分享機制。 2.導入威脅入侵評估及端點偵測回應服務。 3.紅隊演練。	130,000,000		1.建置系統完成。 2.SOC 收容機關數量達 50%。 3.重要系統異地備份。 4.滲透測試系統達全府核心系統 50%。 5. 本府 GCB 導入機關（A、B 級）比例達 60%。	1
108	1	區域聯防服務	1. 區域聯防維運服務（二線 SOC 監控、戰情中心及威脅入侵服務）。 2. ISAC 建置及維運。 3. 政府組態基準導入服務。	29,248,000	0	1.持續維運二線 SOC 監控、戰情中心及威脅入侵服務。 2.建置 ISAC。 3.本府 GCB 導入機關(A、B 級）比例達 80%。	1
	2	本府資安基礎環境強化	1.異地備援。 2.針對 EOS 設備進行更換。 3.重要系統進行滲透測試、弱點掃描及資安健檢。 4.國際資安證照教育訓練。	30,000,000	9,000,000	1.完成異地備援。 2.完成 EOS 設備進行更換。 3.完成系統進行滲透測試、弱點掃描及資安健檢。 4.完成國際資安證照教	2

年度	項次	工作項目	工作內容	所需經費		績效目標	優先次序（必填）
				經常門	資本門		
						育訓練。	
109	1	區域聯防服務	1.區域聯防維運服務（二線SOC監控、ISAC、戰情中心及威脅入侵服務）。 2.政府組態基準導入服務。	26,760,000	0	1.持續維運二線SOC監控、ISAC、戰情中心及威脅入侵服務。 2.本府GCB導入機關(A、B級）比例達95%。	1
	2	本府資安基礎環境強化	1.異地備援。 2.針對EOS設備進行更換。 3.重要系統進行滲透測試、弱點掃描及資安健檢。 4.國際資安證照教育訓練。	40,000,000	5,000,000	1.完成異地備援。 2.完成EOS設備進行更換。 3.完成系統進行滲透測試、弱點掃描及資安健檢。 4.完成國際資安證照教育訓練。	2
小計				126,008,000	14,000,000		
花蓮縣政府							
108	1	花蓮縣政府資安防護計畫	資安監控中心(SOC)服務-府內 導入政府組態基準(GCB) 府內及一級(B級)機關 導入政府組態基準(GCB) 基層公所	1,555,000	0	SOC持續營運 重要系統完成滲透測試。 弱點掃描 GCB導入達50%。 完成定期資安健診。	1
	2	社政資安防護計畫	老舊(逾七年)設備汰換(個人PC) 老舊(逾七年)設備汰換(個人PC) 107未補足	0	450,000	完成老舊設備汰換。	2
	3	公所資安防護計畫(設備汰換)	(一) 花蓮市公所-老舊(逾七年)設備汰換(個人 PC) 107未補足 (二) 吉安鄉公所-老舊(逾七年)設備汰換(個人PC) 吉安鄉公所-老舊(逾七年)設備汰換(個人PC) 107未補足 (三) 玉里鎮公所-老舊(逾七年)設備汰換(個人PC) 玉里鎮公所-老舊(逾七年)設備汰換(個人PC) 107未補	0	2,773,000	完成老舊設備汰換。	3

年度	項次	工作項目	工作內容	所需經費		績效目標	優先次序（必填）
				經常門	資本門		
			足 (四) 秀林鄉公所-老舊(逾七年)設備汰換(個人PC)				
109	1	花蓮縣政府資安防護計畫	資安監控中心(SOC)服務-府內 資安監控中心(SOC)服務-B級機關 滲透測試 資安健診 導入政府組態基準(GCB) 府內及一級(B級)機關 導入政府組態基準(GCB) 基層公所	3,626,000	0	SOC持續營運重要系統完成滲透測試。 弱點掃描 GCB 導入達95%。 完成定期資安健診。	1
	2	公所資安防護計畫(設備汰換)	(一) 吉安鄉公所-老舊(逾七年)設備汰換(個人PC) (二) 玉里鎮公所-老舊(逾七年)設備汰換(個人PC) (三) 秀林鄉公所-老舊(逾七年)設備汰換(個人PC) (四) 花蓮市政府-老舊(逾七年)設備汰換(個人PC)	0	667,000	完成老舊設備汰換。	2
小計				5,181,000	3,890,000		
金門縣政府							
108	1	虛擬化系統資安強化	1.虛擬化系統分散式防火牆導入 2.虛擬桌面導入	0	1,714,000	建置完成。	1
109	1	資安專用防火牆購置及維護	1.防火牆購置及部署	0	2,314,000	建置完成。	1
小計				0	4,028,000		
連江縣政府							
108	1	設備汰換、資訊安全	1.汰換已使用7年以上之終端設備 2.建置連江縣機房資訊安全專用伺服器 3.防火牆購置	0	4,767,000	完善基礎設施、強化各單位資安節點能量。	2

年度	項次	工作項目	工作內容	所需經費		績效目標	優先次序（必填）
				經常門	資本門		
		專用伺服器及防火牆					
	2	GCB維運	購置授權及持續配合中央GCB導入政策	0	400,000	持續配合中央GCB導入政策。	3
	3	SOC維運及資安健檢	持續委外並配合臺北市區域聯防,完善本縣維運一線SOC功能。	904,000	0	配合台北市執行SOC建置,本府將提報該項並持續維運,在資安人才欠缺的窘境下,仍能完善區域聯防機制下一線SOC功能。	1
109	1	資訊安全專用伺服器及防火牆	1.建置連江縣機房資訊安全專用伺服器 2.防火牆購置	0	1,433,000	完善基礎設施、強化資安各單位節點能量。	2
	2	GCB維運	購置授權及持續配合中央GCB導入政策	0	400,000	持續配合中央GCB導入政策。	3
	3	SOC維運	持續委外並配合臺北市區域聯防,完善本縣維運一線SOC功能。	985,000	0	配合台北市執行SOC建置,本府將提報該項並持續維運,在資安人才欠缺的窘境下,仍能完善區域聯防機制下一線SOC功能。	1
小計				1,889,000	7,000,000		

九、經費補助表

單位：新臺幣元

年度	總經費	其他基金或補助款	地方政府自籌款	行政院補助款
臺北市政府				
107	130,000,000	無	65,000,000	65,000,000
108	68,248,000	無	34,124,000	34,124,000
109	71,750,000	無	35,880,000	35,880,000
花蓮縣政府				
107	4,276,000	無	428,000	3,848,000
108	4,778,000	無	478,000	4,300,000
109	4,293,000	無	429,000	3,864,000
金門縣政府				
107	4,560,000	無	1,368,000	3,192,000
108	1,714,000	無	514,000	1,200,000
109	2,314,000	無	694,000	1,620,000
連江縣政府				
107	3,852,000	無	385,000	3,567,000
108	6,071,000	無	607,000	5,464,500
109	2,818,000	無	282,000	2,536,000

十、預定進度

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
107/4	25%	無	1. SOC 監控月報。
107/7	50%	當年度費用 50%	1. SOC 監控月報。 2. 戰情中心服務月報。
107/10	75%	無	1. SOC 監控月報。 2. 戰情中心服務月報。

108/1	100%	107 年度費用 100%	1. SOC 監控月報。 2. 戰情中心服務月報。 3. 紅隊演練報告。 4. 資安稽核及輔導報告。 5. 資安健診報告。 6. 教育訓練情形。
108/4	25%	無	1. SOC 監控月報。 2. 威脅入侵評估月報。 3. 戰情中心服務月報。
108/7	50%	108 年度費用 50%	1. SOC 監控月報。 2. 威脅入侵評估月報。 3. 戰情中心服務月報。 4. ISAC 區域聯防二線監控系統。
108/10	75%	無	1. SOC 監控月報。 2. 威脅入侵評估月報。 3. 戰情中心服務月報。 4. ISAC 區域聯防二線監控系統。
109/1	100%	108 年度費用 100%	1. SOC 監控月報。 2. 威脅入侵評估月報。 3. 戰情中心服務月報。 4. ISAC 區域聯防二線監控系統。 5. 弱點掃描、滲透測試、資安健診報告。 6. 教育訓練情形。
109/4	25%	無	1. SOC 監控月報。 2. 威脅入侵評估月報。 3. 戰情中心服務月報。 4. ISAC 區域聯防二線監控系統。
109/7	50%	109 年度費用 50%	1. SOC 監控月報。 2. 威脅入侵評估月報。 3. 戰情中心服務月報。 4. ISAC 區域聯防二線監控系統。
109/10	75%	無	1. SOC 監控月報。 2. 威脅入侵評估月報。 3. 戰情中心服務月報。 4. ISAC 區域聯防二線監控系統。
110/1	100%	109 年度費用 100%	1. SOC 監控月報。 2. 威脅入侵評估月報。 3. 戰情中心服務月報。 4. ISAC 區域聯防二線監控系統。 5. 弱點掃描、滲透測試、資安健診報告。 6. 教育訓練情形。

十一、預期效益

(一) 藉由結合區域內資訊安全運作中心（SOC）建立二線 SOC 機制，擴大整體監測可視性、強化防護規則、標準化作業流程並增加防護規則準

確性。

(二) 建構區域資安警訊平台(ISAC)，效益如下：

1. ISAC 監控到之訊息可即時傳遞至 SOC 強化規則防護及提供予 CERT 進行資安事件處理。
2. 各縣市政府得以即時了解資安防護狀態、內外部資安情資，以及早因應類似攻擊方式達到預警功效。

(三) 成立資安事件緊急處理中心，效益如下：

1. 建立區域應變團隊及資安事件應變流程，掌握資安事件處理進度、落實並回饋資安事件處理機制。
2. 及早預防或減緩資安事件影響範圍、藉由區域內其他機關之資安事件透過教育訓練提高機關應變事件能力。

(四) 提升國內資安產業能量：於推動區域聯防中心時，將基礎資安檢測服務、教育訓練及資安前瞻研究納入學界合作範圍，提升資安人才培育及資安研發能量。

十二、相關聯絡資料

單位	聯絡人姓名	電話	E-mail
臺北市政府	李佳怡	02-27208889#2845	ic-chiayi@mail.taipei.gov.tw
花蓮縣政府	潘振光	03-8227171#328	tr8232@hl.gov.tw
金門縣政府	吳宗翰	082-318823#62953	dickson11@mail.kinmen.gov.tw
連江縣政府	曹家輝	0836-23368	chiahui@ems.matsu.gov.tw

附件 4

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之分項計畫

新北市

108年3月

新北市政府
強化政府基層機關資安防護及區域聯防計畫

一、計畫緣起

目前各地方政府資訊主管機關所負責之資訊作業環境複雜、多元、設備眾多（註 1-3），依據「政府機關（構）資通安全責任等級分級作業規定」應辦之工作事項，持續進行電腦防毒保全、資安監控，並每年定期針對重要系統主機進行弱點掃描、滲透測試及資安健診等資安檢測服務，惟近年來國際資安事件頻傳，駭客攻擊手法日新月異，外部資通安全發展則有更前瞻的技術方案，而市府目前多數設備老舊，效能及安全性已不符需求，且因市府資源有限，僅能以逐年分攤方式進行部分電腦主機、防火牆、核心交換器及 IPS 等資訊及資安設備更新及升級，故研提本計畫，綜整市府資安防護不足之部分進行強化，並提升整體資訊服務效能及安全防護能量，同時與基隆市及宜蘭縣政府合作，建立資安區域聯防與跨機關服務合作機制，以符合現行資安環境橫向防禦需求。

又為利提升跨縣市政府合作之資通安全防護能力，規劃提升現有資安設施功能，引進新技術，強化資安防護能力，並優先以國產品牌相關軟硬體設備為採購標的，以促進國內資安相關產業經濟發展。同時引進產業與學術資訊安全專業人員，提高國內資訊安全職能的發展。

註 1：新北市政府有 28 個一級機關、31 個二級機關及 28 個區公所，員工人數約計 45,000 人。
註 2：宜蘭縣政府一級單位共 15 處、6 局，二級機關共 22 個機關，員工人數計約 7,700 人。
註 3：基隆市政府一級單位共 14 處、6 局，二級機關共 23 個機關，員工人數計約 4,300 人。

二、計畫目標

(一) 強化資訊基礎設施安全防護能力：更新縣市政府及所屬機關使用已達 7 年以上之具資安風險資訊軟硬體設備，並以國產品為優先採購。

(二) 落實區域聯防機制：加強資安軟硬體設備佈建及資安檢測服務，提升

資訊安全防護能量，並配合行政院國家資通安全會報技術服務中心運行之政府組態基準（GCB）推動；建立資安快速應變小組，協防所屬縣市及轄下機關提供資安諮詢或技術支援，強化資安監控中心區域聯防運作機制，透過標準化格式，進行跨縣市政府資安資訊分享及交換，以即時通知及提升預防能力，達到區域聯防之效益。

(三) 建立持續營運體係：深化資訊安全管理機制，透過 PDCA 循環，持續完善資安營運體係，由各縣市政府編列常態性公務預算，持續維運相關軟硬體設備及服務，並維持跨縣市區域聯防及合作事項，以達持續營運之目標。

(四) 發展創新 e 化便民服務：建置及強化優質的便民服務，並藉由經驗分享及移植，使服務發展跨越縣市限制，擴展行動化服務宅配到家之服務及推動 ODF 為政府文建標準格式，提升市府機關整體服務效能，提供民眾更友善服務環境。

(五) 促進產官學合作：軟硬體設備汰換以國產資安產品為優先採購標的，並依地方政府發展需求，提供試驗場域，進而提升資安自主產品使用率，同時，借助產業與學界技術專業人力及知識經驗，規劃資安教育訓練相關課程，提升資訊安全知識及能力，以持續帶動國內資安產業發展，提升國內企業資安軟實力。

三、計畫內容與實施策略

(一)　強化資訊基礎設施安全防護能力

為強化各縣市資訊基礎設施安全防護能力，更新使用年限達 7 年以上具資安風險之 6,671 台老舊電腦及伺服主機，並強化基礎資安設備環境，以分年度更新方式執行，符合基礎設備安全防護能力，惟新北市

個人電腦採購作業係統籌本府 263 機關數量，採用租賃服務以公開評選方式執行，該採購方式單台電腦採購金額優於共同供應契約單台電腦金額，因採購法規定無法要求特定來源地、生產者或供應者，故該項採購作業若決標結果若為國外產品，將配合提供行政院資處說明報告。

(二) 落實區域聯防機制

1. 加強資安軟硬體設備佈建，規劃建置及升級 IPS/IDS、WAF、防火牆、防垃圾郵件、SSLVPN、SSL 解碼分析、log 蒐集分析及網路管理等資安軟硬體設備，以健全基礎設施安全防護能量。
2. 規劃進行資訊安全檢測服務包含弱點掃描、滲透測試及資安健檢服務。
3. 建置及維運區域聯防平台：新北市政府統一建置區域聯防系統(包含 ISAC、CERT 及區域 SOC)，並統籌區域聯防機制建立，另透由標準化格式將宜蘭縣及基隆市政府一線 SOC 之資安事件資料收納於新北市區域 SOC 中，透由區域 SOC 整體分析其區域性攻擊事件，以提升區域內防護能力。
4. 建立資安快速應變小組及機制(CERT)，以各縣市政府資安人力參與本區域聯防作業，並由 3 個縣市共同制定機制及流程，當發生重大資安事件時，如資料洩漏、大規模網頁置換、SPAM、中毒事件等，透過本區域聯防作業機制成立資安快速應變小組，協防所屬縣市及轄下機關，提供資安諮詢或技術支援，針對資安事件能即時做出對應的處置，以提升地方政府整體應變能力。
5. 建立跨縣市資安監控區域聯防及資訊分享機制(ISAC)，導入資訊安

全資料蒐集及分析設備，由 3 個縣市共同制定機制及流程，透由 ISAC 蒐集國內外情資、交換及分析，瞭解資安威脅及弱點，發生大規模之網路攻擊時，可針對可能之威脅進行有效預防措施，透過分享資安相關情資與分析資料，以強化整體應變與防護能力。

6. 配合行政院國家資通安全會報技術服務中心運行之政府組態基準（GCB），推動政府 GCB 導入作業，規範資通訊終端設備(如：個人電腦)一致性安全設定(如：密碼長度、更新期限等)，以降低成為駭客入侵管道，進而引發資安事件之疑慮。
7. 基隆市政府規劃逐年辦理各機關行政網路線路收容作業，俾利後續資安區域聯防相關服務推動。

(三) 建立持續營運體系

各縣市政府後續編列公務預算維持營運本計畫相關軟硬體設備及維運作業，持續進行跨縣市區域聯防及便民服務，並不定期辦理跨縣市交流研討會，以達到持續營運目標。

(四) 發展創新 e 化便民服務

1. 數位學習:持續進行服務需求增修，除便民外，亦降低行政處理負荷及提高推行效率以達一站式服務之目標，結合建立 e 化管理機制。
2. e 化便民服務:整合各式功能之服務需求，增加其功能增修及各項維運作業，加速民眾的訊息同步效率，並擴大對民眾的服務範疇，以提升服務之有效性。
3. 透過辦理 ODF 使用操作教育訓練及說明會，持續推動 ODF 文件標準格式，提升 ODF 整體使用率。

(五) 促進產官學合作

1. 宜蘭縣政府將規劃由區域大學(如宜蘭大學)學生參與本專案作業(如

資安檢測)，並邀請該大學資安領域教授提供相關講座與課程。

2. 與產業合作其聯防作業，依地方政府發展需求，提供產學研合作場域，提升資安自主產品使用率，以帶動國內資安產業自主研發能量，提升資安產業軟實力。

四、實施範圍

新北市政府、基隆市政府、宜蘭縣政府（含所屬一級、二級機關及鄉鎮區公所）。

五、計畫期程

民國 108 年 1 月至民國 109 年 12 月。

六、關鍵績效指標及年度目標值

108 年	109 年
1. 資安分享機制交換重要資安訊息每年 80 則。 2. 政府組態基準設定(GCB)導入 B 級機關導入作業達 80%。 3. 基隆市累計完成 29 個機關線路整併作業。 4. 提供產學合作場域，視資安產品優劣進行推薦。 5. 提升資安自主產品使用。 6. 健全資安檢測服務，至少完成下列項目: （1）系統弱點掃瞄：2,000 次。 （2）網頁弱點掃描：340 次。 （3）滲透測試：15 次。 （4）資安健診：100 人天。	1. 持續運作及精進資訊分享系統(ISAC)及緊急應變通報(CERT)機制。 2. 資安分享機制交換重要資安訊息每年 100 則。 3. 政府組態基準設定(GCB)導入 B 級機關導入作業達 95%。 4. 基隆市累計完成 34 個機關線路整併作業。 5. 提供產學合作場域，視資安產品優劣進行推薦。 6. 提升資安自主產品使用。 7. 健全資安檢測服務，至少完成下列項目: （1）系統弱點掃瞄：2,000 次。 （2）網頁弱點掃描：340 次。 （3）滲透測試：15 次。 （4）資安健診：100 人天。

七、持續營運評估

(一) 經費來源：計畫期滿後由各縣市政府自行編列公務預算，持續維運本計畫軟硬體設備及服務項目。

(二) 完善聯防機制：計畫期滿後由各縣市政府自行編列公務預算，持續維運本計畫軟硬體設備及服務項目。

(三) 產學合作: 與產業合作其聯防作業，並提供產學研合作場域，帶動國內資安產業自主研發能量，提升資安軟實力。

八、經費明細概算

本計畫預估總經費如下:

政府機關	108 年度	109 年度	合計
新北市政府	73,575,000	129,058,000	202,633,000
宜蘭縣政府	67,875,000	29,125,000	97,000,000
基隆市政府	38,571,000	47,600,000	86,171,000
合計	180,021,000	205,783,000	385,804,000

(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		
	1	建置及提升資安防護軟硬體設備	更新交換器	2,250,000	0	更新老舊交換器設備	2
			安裝防毒機制	800,000	0	提供更新老舊資訊之設備防毒防護服務	
			加裝防火牆	4,900,000	0	行政網路環境擴增及汰換防火牆	
			資產管理系統	1,392,000	0	維運資產管理系統	
			網路管理工具	0	6,000,000	建立網路管理機制	

	2	提供資安防護服務	弱點掃描服務	800,000	0	提供弱掃服務	3
			滲透測試服務	800,000	0	提供滲透測試服務	
			資安健診服務	800,000	0	提供資安健診服務	
			APT 服務	800,000	0	提供 APT 服務	
			辦理 ISMS 制度推廣認證	238,000	0	ISMS 認證制度推動	
			導入政府組態基準(GCB)	840,000	0	推動政府組態基準(GCB)，強化資訊基礎設備安全性	
			系統資安防護服務	0	3,500,000	強化個人資料保護服務	
	3	雲端資訊資源服務	雲端資訊資源服務	2,621,000	3,992,000	強化雲端資訊資源服務	5
	4	異地備份或備援機制	維運異地備份或備援機制	4,266,000	0	建立異地備份或備援機制，提高系統安全保護及服務可用性	6
	5	區域聯防系統維運	維運區域聯防監控服務機制	5,402,000	0	維運區域聯防系統	1
	6	提供創新服務服務	e 化便民服務	3,736,000	508,000	發展 e 化便民服務	7
	7	促進產官學合作	產學合作場域	500,000	0	產學合作場域	4
小計				30,145,000	14,000,000		
109	1	更新具風險之資訊設備	更新 7 年以上資訊設備	0	2,070,000	更新老舊電腦	7
	2	裝置及提升資安防護軟硬體設備	更新交換器	7,200,000	6,500,000	更新老舊交換器設備	2
			安裝防毒機制	800,000	0	提供更新老舊資訊之設備防毒防護服務	

			加裝防火牆	6,200,000	0	行政網路環境擴增及汰換防火牆	
			加裝 IPS/IDS 設備	0	12,071,000	維運 IPS/IDS 資安防護設備	
			資產管理系統	1,392,000	0	維運資產管理系統	
			網路管理工具	7,812,000	2,500,000	強化網路管理系統	
			維運 log 蒐集分析服務	0	4,975,000	維運及強化 log 蒐集及分析服務	
	3	提供資安防護服務	提供弱點掃描服務	800,000	0	提供弱掃服務	3
			提供滲透測試服務	800,000	0	提供滲透測試服務	
			提供資安健診服務	800,000	0	提供資安健診服務	
			提供 APT 服務	800,000	0	提供 APT 服務	
			辦理 ISMS 制度推廣認證	308,000	0	ISMS 認證制度推動	
			導入政府組態基準(GCB)	2,207,000	0	推動政府組態基準(GCB)，強化資訊基礎設備安全性	
			系統資安防護服務	617,000	0	強化個人資料保護服務	
	4	雲端資訊資源服務	雲端資訊資源服務	2,895,000	6,000,000	強化雲端資訊資源服務	5
	5	異地備份或備援機制	維運異地備份或備援機制	3,285,000	0	建立異地備份或備援機制，提高系統安全保護及服務可用性	6
	6	區域聯防系統維運	維運區域聯防監控服務機制	5,402,000	0	維運區域聯防系統	1
	7	提供創新服務服務	e 化便民服務	750,000	751,000	e 化便民服務	8

	8	促進產官學合作	產學合作場域	500,000	0	產官學合作發展	4
小計				42,568,000	34,867,000		
合　　計				121,580,000			

(二)　**宜蘭縣政府**

年度	項次	工作項目	工作內容	所需經費(元)		績效目標	優先次序
				經常門	資本門		
108	1	更新具風險之資訊設備	個人電腦(汰換/新增)	0	2,016,000	汰換7年以上之個人電腦	8
			伺服器汰換(虛擬主機)	0	14,476,000	集中建置虛擬主機提供本府與所屬使用	6
	2	裝置及提升資安防護軟硬體設備	防火牆	0	11,640,000	汰換本府與所屬防火牆服務	9
			資料庫稽核系統	0	2,500,000	建置本府資料庫稽核系統	10
			網站式應用服務防火牆(WAF)	0	2,500,000	建置本府WAF供本府與所使用	13
			路由器/交換器汰換	0	8,175,000	建置本府路由供本府與所屬使用	11
			IP管理	0	654,000	建置所屬機關IP管理服務，導入衛生局與文化局	14
			網路管理_SSL加解密	0	6,263,000	建立本府GSN/VPN加解密服務，以利網路設備進行資安管理。	3
			VPN遠端管理	0	1,051,000	建立本府VPN服務，以利進行遠端管理。	12

			防毒系統服務	1,206,000	0	建立本府與所屬防毒系統服務	15
			建立本府與所屬資產管理系統服務	1,056,000	0	建立本府與所屬資產管理系統服務	16
			虛擬主機與異地備份授權服務	1,107,000	0	提供虛擬主機管理、防毒、備份等授權服務	7
			GSN/VPN 對外網路頻寬升級	1,459,000	0	提升本府GSN/VPN對外頻寬	4
			推動 ODF 文件標準	2,146,000	0	推動標準化文件使用	5
	3	提供資安防護、審查、監看機制	封包側錄軟體	0	2,600,000	建立本府封包側錄服務，以利進行資安管理。	2
			資安監控中心(SOC)服務	1,430,000	0	區域聯防資安監控中心(SOC)服務	1
小計				**16,000,000**	**45,875,000**		
109	1	更新具風險之資訊設備	個人電腦(汰換/新增)	0	3,192,000	汰換7年以上之個人電腦	6
	2	裝置及提升資安防護軟硬體設備	防火牆	0	2,352,000	汰換本府與所屬防火牆服務	7
			路由器/交換器汰換	0	3,581,000	建置本府路由供本府與所屬使用	8
			防毒系統服務	2,438,000	0	建立本府與所屬防毒系統服務	9
			資產管理服務	545,000	0	建立本府與所屬資產管理系統服務	10

			虛擬主機與異地備份授權服務	6,120,000	0	提供虛擬主機管理、防毒、備份等授權服務	5
			GSN/VPN 對外網路頻寬升級	2,040,000	0	提升本府GSN/VPN 對外頻寬	3
			推動 ODF 文件標準	3,000,000	0	推動標準化文件使用	4
	3	提供資安防護、審查、監看機制	資安監控中心(SOC)服務	3,607,000	0	區域聯防資安監控中心(SOC)服務	2
			GCB(導入政府組態基準設定)(含 GCB 導入工具)	2,250,000	0	導入政府組態基準設定	1
小計				20,000,000	9,125,000		
合　　計				**97,000,000**			

(三)　**基隆市政府**

年度	項次	工作項目	工作內容	所需經費(元)		績效目標	優先次序
				經常門	資本門		
108	1	更新具風險之資訊設備	汰換 7 年以上之個人電腦	0	6,350,000	更新台老舊電腦 254 台	6
			建置集中式虛擬化伺服主機平台	0	4,290,000	汰換老舊伺服器，建置集中式虛擬化伺服主機平台服務供本府及基層機關使用。	
	2	裝置及提升資安防護軟硬體設備	設置(汰換)資安防護設備)	0	2,582,000	汰換防火牆、WAF、IPS、APT 等資安防禦設備	7
			建置共用郵件伺服器及垃圾郵件防治機制	0	3,201,000	建置垃圾郵件防治機制	

	3	提供資安防護服務	進行弱點掃描服務	155,000	0	針對基隆市政府及所屬機關進行弱點掃描、滲透測試、資安健診及推動ISMS。	10
			進行滲透測試服務	375,000	0		
			進行資安健診服務	2,444,000	0		
			進行 ISMS 機制推廣	991,000	0		
			資安監控中心(SOC)服務及區域聯防平台介接	2,643,000	0	資安監控中心(SOC)服務、區域聯防平台介接。	1
			進行 GCB 導入	991,000	0	執行本府及 108 年度線路整併機關 GCB 導入作業。	8
			推動 ODF 文件標準服務	330,000	0	推動 ODF 文件標準服務。	9
	4	所屬機關行政網路線路整併收容作業	線路整併機關網路架構及終端設備調設定	1,123,000	0	持續針對所屬基層機關進行線路整併收容作業。	2
			調整網路安全管控措施(VPN 遠端管理、SSL 加解密管理、無線網路管理、AD 調校等)	2,661,000	0	配合線路整併規劃調整本府網路安全管控措施	3
			裝置防毒軟體、資產管理軟體、EDR、IP 控管軟體等端點管控措施	6,858,000	0	配合線路整併作業針對納管之設備進行端點管控措施。	4
			建置行政共通系統	0	3,577,000	建置員工入口網等共用行政系統，減少系統散落開發風險。	5
小計				18,571,000	20,000,000		
109	1	更新具風險之資訊設備	汰換 7 年以上之個人電腦	0	3,025,000	汰換個人電腦 121 台	5
			建置集中式虛擬化伺服主機平台	0	4,369,000	汰換老舊伺服，建置集中式虛擬化伺服主機平台服務供本府及基層機關使用。	

	2	裝置及提升資安防護軟硬體設備	設置(汰換)資安防護設備)	0	7,438,000	汰換防火牆、WAF、IPS、APT 等資安防禦設備	7
			建置共用郵件伺服器及垃圾郵件防治機制	0	1,727,000	建置垃圾郵件防治機制	
			日誌系統建置	0	5,184,000	建置日誌管理系統	
	3	提供資安防護服務	進行弱點掃描服務	224,000	0	針對基隆市政府及所屬機關進行弱點掃描、滲透測試、資安健診及推動 ISMS。	8
			進行滲透測試服務	541,000	0		
			進行資安健診服務	3,533,000	0		
			進行 ISMS 機制推廣	2,578,000	0		
			資安監控中心(SOC)服務及區域聯防平台介接	3,820,000	0	資安監控中心(SOC)服務、區域聯防平台介接。	1
			進行 GCB 導入	1,432,000	0	執行本府及 109 年度線路整併機關 GCB 導入作業。	9
			推動 ODF 文件標準服務	480,000	0	推動 ODF 文件標準服務。	10
	4	所屬機關行政網路線路整併收容作業	線路整併機關網路架構及終端設備調設定	1,623,000	0	持續針對所屬基層機關進行線路整併收容作業。	2
			調整網路安全管控措施(VPN 遠端管理、SSL 加解密管理、無線網路管理、AD 調校等)	2,000,000	0	配合線路整併規劃調整本府網路安全管控措施	3
			裝置防毒軟體、資產管理軟體、EDR、IP 控管軟體等端點管控措施	6,626,000	0	配合線路整併作業針對納管之設備進行端點管控措施。	4
			建置行政共通系統	0	3,000,000	建置員工入口網等共用行政系統，減少系統散落開發風險。	6
小計				22,857,000	24,743,000		

	86,171,000

註：

1. 本表可依需求增列。
2. 請詳列各工作內容、經費編列及對應績效目標，多項工作對應單一績效目標時，請於備註欄說明。

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	行政院資通安全處補助款
108	73,575,000		29,430,000	44,145,000
109	129,058,000		51,623,000	77,435,000
合計	202,633,000		81,053,000	121,580,000

(二) 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(20%)	行政院補助款
108	67,875,000		13,575,000	54,300,000
109	29,125,000		5,825,000	23,300,000
合計	97,000,000		19,400,000	77,600,000

(三) 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(30%)	行政院資通安全處補助款
108	38,571,000		11,571,000	27,000,000
109	47,600,000		14,280,000	33,320,000
合計	86,171,000		25,851,000	60,320,000

十、預定進度

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點

108 年	46.67%	180,021,000	1. 持續 B 級機關 GCB 導入作業。 2. 更新老舊資訊設備及佈署防毒機制。 3. 維護防火牆、防垃圾郵件、資產管理、網路管理等軟硬體設備。 4. 資安檢測服務，駭侵事件處理。 5. 基隆市持續進行機關線路整併作業。 6. 提供國內企業資安產品實驗場域，視資安產品優劣進行推薦 7. 提升自主產品使用。 8. 發展及推廣創新 E 化便民服務。
109 年	100%	385,804,000	1. 維持區域聯防資安情資分享機制。 2. 持續 B 級機關 GCB 導入作業。 3. 更新具風險之老舊資訊設備及佈署防毒機制。 4. 維護防火牆、防垃圾郵件、資產管理及網路管理等軟硬體設備。 5. 資安檢測服務，駭侵事件處理。 6. 基隆市持續進行機關線路整併作業。 7. 提供國內企業資安產品實驗場域，視資安產品優劣進行推薦 8. 提升自主產品使用。 9. 發展及推廣創新 E 化便民服務。

十一、預期效益

(一) 強化資訊基礎設施安全防護能力

1. 完備各機關關鍵基礎設施，強化資安防護能力。
2. 使用國內資安產品，帶動國內資安產業自主研發能量，促成我國資安產業發展。
3. 規範使用者設備一致性安全設定，提供高安全性之公務作業環境，保護機敏公務資料。

(二) 落實區域聯防機制

1. 完善資安區域聯防體系，健全資安防護及提升整體應變能力。
2. 資安情報分享，擴大關聯分析的範圍，洞察潛在危機，增加防禦深度，倍增資安防禦力。

3. 資源有效利用及共享，減少建置資安設備及人力成本。

(三) 建立永續營運體系

1. 制度化資安治理流程，深化資訊安全制度。

2. 健全資安預算編列，永續營運及精進。

(四) 發展創新 e 化便民服務

1. 擴展行動 e 化宅配到家服務，藉由整體規劃及流程整合再設計，提升基層機關整體服務效能。

2. 全面推動 ODF 文件標準格式，確保跨機關文件相容性。

(五) 促進產官學合作

1. 資安防禦經驗分享及防禦技術交流，汲取各產業資安新知，以因應日新月異的資安攻擊手法。

2. 提升國內資安產品使用，持續帶動國內資安產業發展，進而提升國際競爭力。

3. 提供產學研合作場域，推薦優質之資安產品，帶動國內資安產業自主研發能量，提升資安軟實力。

十二、相關聯絡資料

機關單位	聯絡人姓名	電話	E-mail
新北市政府資訊中心	陳暖芬	02-29603456#8526	aj5269@ntpc.gov.tw
新北市政府資訊中心	陳彥彰	02-29603456#8518	ae8332@ntpc.gov.tw
新北市政府資訊中心	黃欣樺	02-29603456#8517	ah3321@ntpc.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-land.gov.tw
基隆市政府 研考處	吳信東	02-24201122#1230	kl947@mail.klcg.gov.tw
基隆市政府 研考處	林志威	02-24201122#1241	a52531@mail.klcg.gov.tw
基隆市政府 研考處	藍家伶	02-24201122#1225	lannew@mail.klcg.gov.tw

附件 5

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之分項計畫

桃園市

108年3月

桃園市政府
108 年-109 年度強化政府基層機關資安防護及
桃竹竹苗區域聯防計畫

一、 計畫緣起

因資訊電子化的日增，政府與產業依賴電腦資訊系也越深，資訊安全成為現代國家安全的重要環節，且配合行政院 106 年 4 月 5 日核定通過之「前瞻基礎建設計畫」，其中「數位建設」子項目「強化政府基層機關資安防護及區域聯防」須提出競爭型計畫以爭取中央補助，本府為提升地方政府資安防護能量，期藉由實質經費補助，促進資通安全相關軟硬體建設之發展，提升資通安全管理效能，加強資安防護縱深機制，進而健全資安防護網，達成厚植自我防護能量，爰結合新竹縣、新竹市及苗栗縣等鄰近區域縣市政府共同提案以強化基層資安防護，提升基層機關之資訊服務能量、建置區域資安聯防、加強資安防禦縱深及創新服務整合。

本府結合新竹縣、新竹市及苗栗縣等鄰近區域縣市政府預定於 107 年完成區域聯防機制部署並試營運數個月，自 108 年起則研提持續營運規劃，亦即區域聯防機制之持續監控維運，以及執行前一計畫之工作項目，期能提升區域整體資安防護力，並與 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，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，本府自 107 年起結合新竹縣、新竹市及苗栗縣等鄰近區域縣市政府部署有效的資安區域聯防機制，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 年則是主要針對 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規劃後續之監控維運、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，完備國家資安基礎建設，其中並包含因應縣市資安縱深防護需求與資安管理法及其子法規定，賡續導入 GCB 端點管控機制、輔導建立資訊安全管理制度及相關規範、TY-ISAC 情資分享平台改版通過無障礙標章案、資訊系統源碼檢測等。此外，除了延續前一計畫已研提之創新服務外，另加入網站程式碼檢測平台、雲端化資訊安全整合平台建置、端點威脅監控維運服務等創新服務。詳如下列說明：

1. 區域資安聯防監控網及技術資源建置共享之監控維運

(1)市網/縣網網路整併。

(2)二線 SOC 區域聯防監控維運。

(3)一線 SOC 監控服務。

(4)ISAC 區域聯防情資系統監控維運。

(5)ISAC 區域聯防防護規則管理與派送系統維運。

2. 資安事件快速應變小組(CERT)監控維運

(1)資安快速應變小組維運。

(2)事件通報處理維運。

(3)資訊安全教育訓練。

(4)結合地區大學能量合作。

3. 賡續強化基層機關資安防護體質，完備國家資安基礎建設

(1)縣市自提資安縱深防護需求。

(1.1)賡續導入 GCB 端點管控機制。

(1.2)建立資訊安全管理制度。

(2)系統資料異地備份(新竹市政府)。

(3)創新服務:

(3.1)弱點掃瞄管理系統共同平台(國內自主研發) (新竹縣政府)。

(3.2)推動 ODF 為政府文件標準格式(新竹縣政府)。

(3.3)行動 APP 檢測認證(國內自主研發) (新竹縣政府)。

(3.4) APT 巨量資料分析設備(國內自主研發) (新竹縣政府)。

(3.5)網站程式碼檢測平台(新竹市政府)。

(3.6)雲端化資訊安全整合平台建置(新竹市政府)。

(3.7) HTTPS 加解密設備(新竹市政府)。

(4)端點威脅監控維運服務。

(5)TY-ISAC 情資分享平台改版通過無障礙標章案。

(6)資訊系統源碼檢測。

三、區域內縣市政府資安現況

依據行政院 107 年 11 月 21 日院臺護字第 1070213547 號令訂定發布資通安全管理法之子法「資通安全責任等級分級辦法」，各等級應有相關規定之作業，因行政院尚未核定，區域聯防所含括之桃園市政府、新竹市政府、新竹縣政府、苗栗縣政府均暫定屬於 B 級。

1. 桃園市政府(資安等級屬 B 級)

共通機房已完成資訊系統分類分級、ISMS 推動作業、防護縱深(防毒、防火牆、郵件過濾裝置、IDS/IPS、Web 應用程式防火牆、APT 攻擊防禦)、監控管理(SOC 監控)、安全性檢測、資安教育訓練等作業，並持續提供相關資安服務與作業。

2. 新竹市政府(資安等級屬 B 級)

B 級機關規定應辦相關工作事項，本府已遵循辦理並陸續建置資安相關防護設備，108-109 年將繼續強化關鍵資訊基礎設施，並落實區域聯防監控，此外並將配合資安法之導入，建立本府資訊安全管理制度，並依

據資通安全責任等級應辦事項之防護措施，進行政府組態基準導入、核心系統驗證、弱點掃描、滲透測試、資安健診、資通安全防護等管控措施，以強化本府網路資訊安全。

3. 新竹縣政府(資安等級屬 B 級)

B 級機關規定應辦相關工作事項，本府已遵循辦理並陸續建置資安相關防護設備，經盤點本縣各機關資訊(安)現況，約 1000 台個人電腦、資訊系統軟硬體老舊急需汰換需約 2269 萬元)、資安與網路設備及資安防護系統汰換建置約 1 億元，故總計約 1 億 3,800 萬元整。

4. 苗栗縣政府(資安等級屬 B 級)

B 級機關規定應辦相關工作事項，本府已遵循辦理並陸續建置資安相關設備，因應本計畫盤點本縣各機關資訊(安)現況，本縣需汰換個人電腦計 1550 台、伺服器主機計 120 台、資安設備汰換計 15 台及網路設備汰換計 40 台(汰換經費約 1 億元)，另配合聯防需求辦理相關建置費用約 4000 萬元，總計約 1 億 4,076 萬元整。

桃園及鄰近縣市政府已於 107 建立二線 SOC、CERT、ISAC 等區域聯防機制，未來若本區域有相關的資訊安全事件出現，將偕同處理，並相關的情資資訊及規則，發布給區域內的縣市政府，已達到共同防護功效。

四、 計畫內容與實施策略

1. 區域資安聯防監控網及技術資源建置共享之監控維運

(1) 市網/縣網網路整併

(一) 內容

為極力發展相關市政/縣政系統及資訊基礎建設，並持續網路整併及調整，以期發展共通系統，減少開發及維運成本，亦可提升網路服務品質。

- 重新切割網段落實 DMZ 及 intranet 網段區隔。
- 為確保府內終端設備與核心系統漏洞保護與進階攻擊能有所保護與防範，將導入端點監控管理機制，除可提供網路監控服務，並可有效降低網路與端點的使用風險，中斷制止惡意勒索軟體，早期預警網

路惡意攻擊行為。

- 藉建立身分識別、存取管理等相關的資安防護與派送服務機制，為府外連線至府內網路之資訊安全嚴格把關。
- 因應網路整併，府內網路相關設備及整併機關之防火牆、網路設備等亦應配合提升效能，為降低硬體設備損壞或資料遺失，進而提高資訊系統之可用性，實須加以汰換過於老舊設備。
- 因應網路整併網段重新切割，機房線路將重新串接，藉由本計畫視需要一併改良老舊無法上鎖、沒有線槽之機櫃，以確保電機房資訊設備及資料安全。
- 新竹市政府：因應網路整併針對府外單位尚未納入 AD 網域控管之單位逐步整合 USER 端安全防護機制，以強化 user 端之資訊安全。此外，因網路整併逐步將本府相關單位 DNS Server 指向本府統一之 DNS Server，因該設備過於老舊且為直立式設備，非標準機架式設備，擬透過本案汰換以強化其負載能力。

(二) 實施策略

- 網段架構調整並重新切割。
- 導入端點監控管理機制及身分識別認證上網機制。
- 汰換無網管功能之 switch。
- 因應網路整併線路調整，擴充府內網路相關設備及整併機關之防火牆、網路設備。
- AD 網域及 DNS 整合，並導入 USER 端安全防護機制。
- 逐步將府外單位納入府內終端防護控管。

(2) 二線 SOC 區域聯防監控維運

藉由 SOC 區域聯防二線監控系統，將各機關的 SOC 資安事件單收容，可對資安事件做跨機關的進階式規則分析，找出各機關的類似攻擊事件，判定駭客的攻擊趨勢與走向，達到區域聯防監控的目標。

(一) 內容

藉由 SOC 區域聯防監控系統，以對區域內的資安威脅做整體分析。

(二) 實施策略

- 以本府為核心藉由 107 年部署完成之二線 SOC 區域聯防監控系統，收容新竹市、新竹縣及苗栗縣政府等區域範圍內機關一線 SOC 資安監控之通報事件單(Event Log)，將事件單資訊一併回傳至技服中心進行二線監控。
- 對機關通報事件進行整合，彙整安全設備日誌與做關聯式分析。
- 依照技服中心二線監控月報格式，定期產出區域資安事件統計報表。

(3) 一線 SOC 監控服務

(一) 內容

針對本府重要網段及設備，執行 7*24 小時全年無休之即時監控管理服務，包括日誌(Log)分析、警訊判讀、事件通報、處理建議等。

(二) 實施策略

- 至少須提供 SOC 監控服務-中流量，受監控的網路整體處理效能可達 2300 EPS(Event Per Second)。
- 勘查本府現有網路環境與需求，部署監控必要之遠端偵測器（如日誌收集器）。
- 資安威脅預警：蒐集國內外資安組織之資安威脅情資，至少包括資安聯防情資、病毒資訊警訊、系統弱點公告、網頁攻擊資訊、新聞事件。

(4) ISAC 區域聯防情資系統監控維運

(一) 內容

分享資安防護規則(如防火牆規則、IPS/IDS 偵測規則等)與攻擊活動訊息(如可疑郵件主旨列表、可疑連線 IP、惡意留言等)，發生大規模

之網路攻擊(如 DDoS、勒索軟體、蠕蟲發作等)時，即時通知所屬鄰近縣市進行預防或增設阻擋規則。

(二) 實施策略

- ISAC 區域聯防情資系統，呈現分析區域內的資安狀況，並於資安平台呈現整體趨勢分析及資安攻擊板塊。
- 透過情資的蒐集、交換及分析，了解本區域之資安威脅與攻擊事件資訊，並提供分析結果與對策，針對可能之威脅進行有效預防措施；此外，並與 N-ISAC 平台進行情資交流，強化情資分享與協調聯防機制，透過分享資安相關情資與分析報告，以利決策者與資安防護人員有效因應資安事件。

(5) ISAC 區域聯防防護規則管理與派送系統維運

(一) 內容

藉由 ISAC 區域聯防防護規則派送系統，將 ISAC 分析所得之防護規則或惡意中繼站清單自動化派送至區域縣市政府之區域聯防設備，以達到區域聯防目的。

(二) 實施策略

以本府為核心，運用 107 年部署之 ISAC 區域聯防防護規則派送系統，當有新惡意中繼站或新攻擊模式出現，經由情資系統分析確認後，即可對受管控之區域聯防資安設備進行防護規則派送。

2. 資安事件快速應變小組(CERT)監控維運

發生重大資安事件時(如資料洩漏、大規模網頁置換、SPAM、中毒等)，透過資安快速應變小組，協防區域聯防鄰近縣市並提供資安諮詢或技術支援，並負責日常 ISAC 維運、資安情資交換運作、及派送阻擋規則，以及對應

各級機關資安人員建立三級資安風險應變制度及專家顧問諮詢。

(1) 資安快速應變小組維運

(一) 內容

本府於區域聯防中心內成立【資安快速應變小組】，主要任務為【SOC/ISAC 平台維護】、【二線 SOC 分析監控】、【ISAC 事件處理與鑑識】、【產學合作訓練與研發】，以協防所屬鄰近縣市在重大資安事件發生後執行緊急應變、入侵管道定位、受影響範圍評估及回復受駭系統。

(二) 實施策略

○ 各主要任務說明如後：

(1) 【SOC/ISAC 平台維護】：負責情資發布及事件通報與規則派送。

(2) 【二線 SOC 分析監控】：負責收集外部及 B/C 級情資進行情資分析。

(3) 【ISAC 事件調查與鑑識】：負責資安應變程序及情資諮詢

(4) 【產學合作訓練與研發】：負責辦理產學合作實習教育訓練及協調實習人員支援 ISAC 執行資安事件調查與鑑識。並協助推動資訊安全相關研究計畫。

○ 區域聯防中心部署後，將建立相關制度，並建立協助支援作業之標準作業流程 SOP，以協防所屬鄰近縣市在重大資安事件發生後執行緊急應變、入侵管道定位、受影響範圍評估及回復受駭系統。

○ 依照「國家資通安全通報應變作業綱要」規定，若為「4」、「3」級事件，將請「資安事件快速應變小組」8 小時內前往協助處理。

(2) 事件通報處理維運

當遭遇勒索病毒或及大規模流量之分散式阻斷服務攻擊等科技犯罪型態

之資安事件，結合所屬鄰近縣市調查處、電腦緊急應變組織，及刑大科技犯罪偵查隊等協防受理通報及處理。

(3) 資訊安全教育訓練

(一) 內容

為提升全民資安意識，可自學生階段即加強資訊安全教育訓練，並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，以培養各級機關資安專業人才為核心，藉由實務操作演練、持續教育訓練，厚植機關人才資源，逐步建立資安自主作業能量。

(二) 實施策略

○ 課程內容與預期目標

針對機關資安人員實施教育訓練，目的在幫助資安人員瞭解最新的資安技術以強化資訊安全防護能力。此外，為了能使各機關資安防護系統管理者熟悉監控設備相關系統操作，規劃提供相關系統功能及運作機制之教育訓練課程，目的在協助各級機關資安人員迅速熟悉相關 SAC 系統平台功能操作及運作機制，更能有效率地控管各式資安事件。課程內容設計將以提升學員參與程度，並提升講師與學員之互動程度為主要考量，藉以提升學習效果。

○ 教育訓練方式

教育訓練分為「資安情資監控教育訓練」與「資安專業訓練」，前者於維運期間，每年度安排機關平台操作管理相關之教育訓練；並安排各課程一次性之外部資安專業訓練，其目的在於提供強化資安工作、提升資安管理所需之專業認證教育訓練。

(4) 結合地區大學能量合作

(一) 內容

資安服務與技術研發為國家之重點發展項目,因應未來國家資安產業擴展須持續補充資訊安全人力之需求,且因資訊安全技術及駭客攻擊手法的演進日新月異,技術門檻高,資訊安全人才之招募與養成不易,故藉由本專案與學術機構合作,透過產業實習計畫的方式,及早尋找並培養有潛力之資安人才,以壯大國家之資安能量。

為培育機關所需之資通訊安全專業人才,鼓勵公私立大學校院曾受過資通安全學程訓練之學生參與前瞻計畫區域聯防規劃,體驗資通安全實務,並透過現場的訓練與操作程序,落實「學以致用」的目標,以強化資訊安全人力的不足,並期使民眾能有機會親身參與了解前瞻計畫資安聯防推展之目的與效益。例如桃園市國立中央大學、新竹市交通大學等,對於新型態威脅攻擊及與國際資安情資交流等均樂於挑戰。

(二) 實施策略

有關資安產學合作之執行方式,可規劃分為短期與長期兩類作業方式,分述如下:

- 短期產學合作實習

  透過與中華民國資訊安全協會合作,可於每年度暑期提供實習名額,期程可視狀況進行調整。

- 長期產學合作實習

  針對於機關暑期實習表現優異之學生或透過校園徵才方式,延攬資安人才,由機關及本計畫委外廠商提供工作機會及獎助學金,預計以一年一約方式進行,期程可視狀況進行調整,至實習生完成學業為止

3. 賡續強化基層機關資安防護體質,完備國家資安基礎建設

(1) 縣市自提資安縱深防護需求

(1.1)賡續導入 GCB 端點管控機制。

(一) 內容

政府組態基準(GCB)目的在於規範資通訊終端設 備(如：個人電腦)的一致性安全設定(如：密碼長度、更新期限等)，以降低成為駭客入侵管道，進而減少引發資安事件之疑慮。有鑑於地方政府經費有限，長年以來資訊設備難以更新，以致部分個人電腦或伺服器作業系統已無原廠維護或無法更新，對於整體資安防護潛藏風險，故應對現有資訊設備先進行全面盤點及汰換，考量所需經費甚鉅，本計畫僅優先針對設備老舊無法導入 GCB，作業系統為 XP、Vista、WIN7 之 PC，不含作業系統為 window server 2000、2003 之伺服器。

(二) 實施策略

- 導入政府組態基準，提列以已無原廠維護或無法更新之個人電腦或作業系統(7 年以上)
- GCB 政策模擬環建立與導入測試。
- 例外清單確認。
- 導入建置。
- GCB 政策回傳機制設定。
- GCB 導入抽測。

(1.2)建立資訊安全管理制度

(一) 內容

建立資訊安全管理制度(Information Security Management System，ISMS)是一套有系統地分析和管理資訊安全風險的方法， ISO27003 是新的 ISMS 標準。各組織對 ISMS 的導入使用規劃(Plan)、執行(Do)、檢查(Check)、行動(Action)四個步驟(簡稱：PDCA)循環，透過風險評估，鑑別出對資產的威脅，估計發生的脆弱點和可能發生性，預測潛在的影響。 以降低成為駭客入侵管道，進而引發資安事件之疑慮。

(二) 實施策略

- 建立資訊安全管理制度。
- 進行驗證。

(2) 系統資料異地備份

(一) 內容

重要業務資訊系統(如本府公文系統)易因無法預期的災害或其他因素導致系統無法正常運行，以及有鑑於日趨頻繁的勒索病毒攻擊事件，更應建立系統資料異地備份以強化備援能力。

(二) 實施策略：

為提升機關行政效率、落實節能減碳、資訊資源向上集中，及緊急災難應變備援能力，朝向規劃系統資料異地備份中心。

(3) 創新服務

3.1 弱點掃瞄管理系統共同平台

(一) 內容

為加強各機關端點資安體質，透過共用弱點掃描檢測平台，使各級機關能有效掌握本身聯外服務之設備是否存在弱點，並能有效自主管理，設定排程進行掃瞄，減少人力介入及便於追蹤管理。

(二) 實施策略

- 為效能考量，縣市政府及區域聯防中心各建置一套弱點掃瞄管理共同平台，並讓定期彙集到區域聯防中心平台內，所有機關皆可自主管理。
- 此平台應具有網頁弱點掃瞄功能、主機弱點掃瞄功能、帳號管理功能、依帳號權限管控所轄主機功能、自主設定主機掃瞄排程、弱點處理/修補回報、弱點自動複檢、弱點豁免簽核等重要追蹤管理功能。

3.2 推動 ODF 為政府文件標準格式

(一)　內容

由地方政府整合所轄基層機關推動 ODF 為政府文件標準格式，藉由統籌辦理相關教育訓練及說明會、研討會等，提升基層機關對 ODF 整體使用效能。

(二)　實施策略

○　提升自由與開源辦公室軟體認知及使用技能

■　每年辦理一次辦理 ODF 開放文件格式宣導及推廣活動，並製作網路線上學習教材，以提昇對 ODF 的認知。

■　每季辦理一次應用軟體操作系列課程，如：簡報(LibreOffice Impress)、試算表(LibreOffice Calc)、文書(LibreOffice Writer)等，機關同仁操作實際體認開源辦公室軟體的好處。

○　提升機關 LibreOffice 自由與開源辦公室軟體安裝比率，協助並教導種子人員安裝軟體。

3.3 行動 APP 檢測認證(國內自主研發)

(一) 內容

行政院國發會將研修「行政院及所屬各機關行動化服務發展作業原則」，增列官方 APP 資安檢測規定，未來新增的官方 APP 都要經資安檢測通過後才能上架。經濟部工業局也將規劃適時將 APP 資安檢測服務納入共同供應採購契約，讓各個政府機關依需求採購 APP 資安檢測服務，確保政府 APP 資安防護。

與民眾生活直接相關的行動APP檢測包含在滲透測試中的一環。檢測內容包含找出伺服器端的漏洞，以及 APP 本身的安全性設定、資料安全、傳輸面等漏洞，行動 APP 檢測通過後，可提供民眾下載時安心使用。

(二) 實施策略

- 盤點已建置的行動 APP。
- 分類一般、存取控制、具有金流功能之數量。
- 預計挑選 5 個進行行動 APP 檢測通過。

3.4 APT 巨量資料分析設備

(一) 內容

APT（進階持續性滲透攻擊）有幾項特色，分別針對了病毒的持續性、針對性、隱匿性、是否為計劃性攻擊攻擊、客製化、攻擊動機以及常見攻擊目標共七個特性。須進行「駭客內網行為分析」在看似正常的系統紀錄中發現不尋常,在繁雜的網路活動紀錄中抽絲剝繭、還原真相;並利用大數據學習系統，不斷進化分析方法，並結合受過 APT 反匿蹤訓練的技術顧問隨時追蹤監控，早期發掘攻擊徵兆，成功擊退入侵者。

在網路封包或資安設備 log 收容後進行大數據資料回溯分析，以創新資安防護思維，藉由回溯分析與巨量資料處理的概念，專注在網路攻擊的控制及擴散行為的偵測，能有效的早期發現潛伏攻擊，提前中斷攻擊路徑，並透過異常行為偵測引擎，持續監控與發掘出潛藏在機關內部的惡意威脅，力求盡量降低機關業務損失、大幅提升地方機關的資安防護能量。

(二) 實施策略

- 建置 APT 巨量資料分析設備。
- 建立具有行為異常察覺、回溯偵測分析、情資導向介面、彈性擴充架構特性的異常行為偵測引擎。
- 提前中斷攻擊路徑效益。

3.5 網站程式碼檢測平台

(一) 內容

原始碼檢測在軟體開發生命週期 (Development Life Cycle) 中扮演著重要的角色。

為加強本府各機關對外網站服務之安全，將導入網站程式碼檢測平台。期望透過平台識別、追蹤和修復軟體原始碼技術上和邏輯方面的安全漏洞。

(二) 實施策略

於本府建置一套網站程式碼檢測平台，讓各機關於系統開發完成或是開發階段即能透過此套系統達到早期發現早期修正程式碼上之安全漏洞，以強化系統之安全及簡少後續程式修復耗費之時間及經費。

3.6 雲端化資訊安全整合平台建置

(一) 內容

雲端技術所帶來的優勢使得企業能夠更為迅速的部署應用程式、降低管理的複雜度和維護的成本，同時允許 IT 資源迅速重新分配以因應企業快速改變的需求。

在虛擬化環境下，伺服器上的軟體架構較傳統架構新增更多層次，且傳統上可透過實體機器將運算工作簡易「分流」的管理方式，也將因虛擬化的採用，必須透過系統管理軟體才能進行管理，一旦虛擬化軟體本身具備安全漏洞，則因單一伺服器上運作的系統因虛擬化採用而較傳統更多，其安全負面影響恐怕也將隨之擴大。

因為虛擬化技術的快速普及，使得系統管理與資訊安全防護也必須因應新的軟硬體布署架構而有所調整，包含建立虛擬化平台與資訊安全系統整合架構，並使用資安或系統管理軟體增加監控的範圍，以預防來自虛擬層的資安漏洞所可能帶來的資安問題。

(二) 實施策略

- 汰換老舊儲存設備主機及硬碟
- 擴充相關授權模組

3.7 HTTPS 加解密設備

(一) 內容

為因應國家發展委員會推動之政府機關導入網站安全傳輸通訊協定，本府以陸續將相關網站服務調整為 Https 加密方式進行資料傳輸。然而，防火牆或 WAF 等既有設備無法將加密的封包解開，雖然傳輸資料採用 SSL 加密確實強化了使用者的資料安全，但卻也造成資安防範的另一個漏洞。為此，期望透過 HTTPS 加解密設備，在解密 SSL 流量的同時維持網路的高效能，並將解密的資料轉送給其他的資安設備(例如防火牆、IPS)來進行深度封包檢測(DPI)，使其與這些防護措施之間，能夠密切地整合，以達到協同防禦的功效。

(二) 實施策略

- 建置 HTTPS 加解密設備
- 對於加密流量，提供政策式的管理與透視能力，而對於後續傳送到既有網路安全設備，進行分析、過濾的流量，能夠藉此更有效地掌控，使其與這些防護措施之間，能夠密切地整合。

4. 端點威脅監控維運服務

(一) 內容

本府 107 年除規劃了一線 SOC 及二線 SOC 監控機制外，有鑑於很多資安威脅或惡意程式係由使用者端設備入侵，故本府除在閘道端規劃有 SOC 監控機制外，並於端點端部署了端點威脅監控軟體，期能雙管齊下，達到更全面性之監控及情資分析。

(二) 實施策略

- 藉由端點所部署之威脅監控軟體及管理平台，回收及分析各端點端所遭遇到之威脅及惡意入侵，以呈現分析區域內的整體資安狀況。

- 透過端點監控程式情資的蒐集及分析，了解本區域之資安威脅與攻擊事件資訊，並提供分析結果與對策，針對可能之威脅進行有效預防措施。

5. TY-ISAC 情資分享平台改版通過無障礙標章案

(一) 內容

依行政院資通安全處 108 年 2 月 18 日院臺護字第 1080164757 號函函送立法院審查中央政府前瞻基礎建設計劃第二期特別預算案數位建設主決議，要求各機關使用前瞻基礎建設計畫之數位建設預算時，所有新設或改版網站，應於 108 年 12 月底前取得「網站無障礙規範 2.0 版」檢測等級 AA 以上之標章，以保障身心障礙者資訊取得之權利，並朝建置更完善無障礙環境邁進。

本府 107 年部署之區域聯防計畫共計新設 1 個網站，網站名稱為「桃竹竹苗區域聯防資安資訊分享與分析中心」(以下簡稱 ty-isac)，擬納入本案計畫執行，依規定於 108 年 12 月底前取得「網站無障礙規範 2.0 版」檢測等級 AA 以上之標章。

(二) 實施策略

- 洽原開發廠商辦理改版以取得「網站無障礙規範 2.0 版」標章。

6. 資訊系統源碼檢測

(一) 內容

隨著網路安全防護意識提昇以及防火牆(Firewall)與入侵防禦系統(IPS)技術的漸趨成熟，駭客將目標漸漸轉向了企業所提供的網站服務，例如企業入口網站、論壇或網路交易平台等。近幾年來，約有 70% 的攻擊是針對 Web 應用程式層(Gartner, 2005)；因此只有保護實體網路是不足的，應用程式也是駭客真正的攻擊目標。不論實體網路的防護做得再好，若應用程式出現漏洞，惡意使用者依然可以輕易的取得

機密資訊。因此在鞏固實體安全的同時，強化應用程式的安全性也同樣舉足輕重。

源碼檢測以檢視原始程式碼的方式,尋找並指出程式中潛藏的安全性弱點，分析其弱點種類、攻擊路徑等資訊；透過分析結果，開發人員可以修改程式以避免弱點產生。爰此，本計畫將針對本府共通性的多個關鍵系統或重要系統執行源碼檢測，期能找出應用程式漏洞，避免惡意使用者可輕易的取得機密資訊，強化系統或網站之資通安全。

(二) 實施策略

洽第三方專業源碼檢測廠商執行檢測服務。

五、 實施範圍

本計畫範圍包含桃園市政府、新竹縣政府、新竹市政府、苗栗縣政府及各縣市政府所屬機關，並依行政院規定以衛政、社政、基層公所等機關為優先實施對象。

六、 計畫期程

本計畫自 108 年起至 109 年止，共計 2 年，並依照行政院補助計畫核可費用實施。

七、 關鍵績效指標及年度目標值

項次	績效指標	評估方式	衡量標準	目標值		
				107	108	109
1	各縣市政府導入基層機關(含衛政、社政及基層公所等)政府組態基準(GCB)	統計數據	各縣市政府(累計設備 GCB 台數/總設備 GCB 建置數)*100%	10%	40%	95%
2	強化資安防護設備，建立區域聯防，各縣市政府減少重大資安事件發生率	統計數據	各縣市政府資安事件數(2 級事件以上)需每年小於 25 件	<=25	<=25	<=25
3	區域聯防協防涵蓋率	統計數據	各縣市政府(區域聯防協防涵蓋機關數/總機關數)*100%	25%	50%	65%

八、 持續營運評估

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預定於107 年完成區域聯防機制部署並試營運後，自 108 年起則研提持續營運規劃，亦即區域聯防機制之持續監控維運，108 年之區域聯防案因原得標廠商無償提供延長服務至 108 年底，故 108 年無需本計畫經費支應，109 年則由本案計畫經費支應，後續行政院若無法繼續補助監控維運經費時，各縣市政府將向機關爭取逐年提列相關維護營運費用以為支應，期能賡續提升區域整體資安防護力，並與 N-ISAC 達到情資分享與建構更為穩固之國家資安監控網。

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。此外，桃竹竹苗之區域聯防建置完成後，亦將建立協助支援作業之標準作業流程 SOP，以協防所屬鄰近縣市在重大資安事件發生後執行緊急應變、入侵管道定位、受影響範圍評估及回復受駭系統等之應變措施。

九、 經費明細概算

單位：新臺幣

年度	項次	工作項目	工作內容	所需經費		績效目標	優先序（必填）
				經常門	資本門		
	一	桃園市政府					
108 年	1	市網/縣網網路整併	預計整併 6 個公所/機關	431,000	10,587,000	汰換基層機關資安設備及網路設備	3
	2-1	導入政府組態基準(GCB)，提列已無原廠維護或無法更新之個人電腦或作業系統(7 年以上)	因不支援新的GCB規則個人電腦	0	36,080,000	汰換基層機關電腦45%以上	1

	2-1-1	導入政府組態基(GCB)端點管控機制	導入GCB端點管控機制	1,690,000	0	導入機關比例75%	2
	2-1-2	輔導建立資訊安全管理制度及相關規範	輔導建立資訊安全管理制度及相關規範、協助取得資通安全專業證照	3,700,000	0	維護本市B級機關資安管理制度。	4
	3	TY-ISAC情資分享平台改版通過無障礙標章案	網站改版通過無障礙標章	500,000	0	取得「網站無障礙規範2.0版」檢測等級AA以上之標章	5
	4	資訊系統源碼檢測	關鍵或重要系統執行應用程式源碼檢測	1,000,000	0	本府共通性的2個(含)以上關鍵系統或重要系統完成源碼檢測	6
108年合計：				53,988,000			
109年	1-1	市網/縣網網路整併	預計整併7個公所/機關	504,000	10,045,000	汰換基層機關資安設備及網路設備	8
	1-2	二線SOC區域聯防監控維運		4,380,000	0	維持區域聯防監系統正常維運	4
	1-3	一線SOC監控服務		1,050,000	0	維持區域聯防監系統正常維	3

						運	
	1-4	ISAC 區域聯防情資系統監控維運		2,400,000	0	維持區域聯防監系統正常維運	5
	1-5	ISAC 區域聯防防護規則管理與派送系統維運		3,006,000	0	維持區域聯防監系統正常維運	6
	2	資安事件快速應變小組(CERT)監控維運	(含資安快速應變小組維運、事件通報處理維運、資訊安全教育訓練及結合地區大學能量合作)	5,009,000	0	維持區域聯防監系統正常維運	7
	3-1	導入政府組態基準(GCB)，提列已無原廠維護或無法更新之個人電腦或作業系統(7年以上)	因不支援新的GCB規則個人電腦	0	28,288,000	汰換基層機關電腦95%以上	1
	3-1-1	導入政府組態基(GCB)端點管控機制	導入GCB端點管控機制	500,000	0	導入機關比例100%	2
	3-1-2	輔導建立資訊安全管理制度及相關規範	輔導建立資訊安全管理制度及相關規範、協助取得資通安全專業證照	1,500,000	0	維護本市B級機關資安管理制度。	9
	4	端點威脅監控維運服務		1,560,000	0	資安國內自主產品	10
109年合計：				58,242,000			

	二	新竹市政府					
108年	1	網路整併費用	關鍵資訊基礎設施強化	759,000	5,130,000	汰換基層機關資安設備	1
	2-1	導入政府組態基準(GCB)，提列以已無原廠維護或無法更新之個人電腦或作業系統(7年以上)	因不支援新的GCB規則個人電腦，伺服器汰換	0	3,220,000	汰換基層機關電腦90%以上	2
	2-2	導入政府組態基(GCB)端點管控機制	導入GCB端點管控機制	1,000,000	0	導入機關比例69%	6
	3-1	建立SOC區域聯防監控系統		1,670,000	0	維持區域聯防監系統正常維運	3
	3-2	成立資安區域聯防中心，與鄰近縣市建立SOC資安聯防機制		2,000,000	0	維持區域聯防監系統正常維運	4
	4	系統資料異地備份		0	3,500,000		7
	5	建立資訊安全管理制度	建立資訊安全管理制度	821,000	0	維護本市B級機關資安管理制度。	5
	6-1	網站安全弱點檢測平台		0	0	資安國內自主產品	10
	6-2	網站程式碼檢測平台		0	0		11
	8	HTTPS加解密設備	針對SSL流量進行解密，並與其他資安設備協同防禦	0	2,400,000		9
	9	雲端化資訊安全整合平台建置		0	3,500,000		8

108 年合計				6,250,000	17,750,000		
109 年	1	網路整併費用	關鍵資訊基礎設施強化	759,000	6,390,000	汰換基層機關資安設備	1
	2-1	導入政府組態基準(GCB)，提列以已無原廠維護或無法更新之個人電腦或作業系統(7年以上)	因不支援新的 GCB 規則個人電腦，伺服器汰換	0	1,610,000	汰換基層機關電腦90%以上	2
	2-2	導入政府組態基(GCB)端點管控機制	導入 GCB 端點管控機制	500,000	0	導入機關比例100%	7
	3-1	建立 SOC 區域聯防監控系統		1,820,000	0	維持區域聯防監系統正常維運	3
	3-2	成立資安區域聯防中心，與鄰近縣市建立 SOC 資安聯防機制		2,000,000	0	維持區域聯防監系統正常維運	4
	4	系統資料異地備份		0	0		8
	5	建立資訊安全管理制度	建立資訊安全管理制度	1,478,000	0	維護本市 B 級機關資安管理制度。	5
	6-1	網站安全弱點檢測平台		0	2,000,000	資安國內自主產品	6
	6-2	網站程式碼檢測平台		0	0		10
	7	APT 巨量資料分析設備	APT 巨量資料分析設備	0	0	資安國內自主產品	9
109 年合計				6,557,000	10,000,000		

	三	**新竹縣政府**					
	1	網路整併費	汰換網路、		5,000,000	汰換基	1

108年		用	資安設備與線路費			層機關資安設備。	
	2-1	導入政府組態基準(GCB)，提列以已無原廠維護或無法更新之個人電腦或作業系統(7年以上)	因不支援新的GCB規則個人電腦,伺服器汰換		15,000,000	汰換基層機關電腦90%以上	2
	2-2	導入GCB端點管控機制	導入GCB端點管控機制	2,500,000		導入機關比例：70%	3
	3	建立SOC區域聯防監控系統		1,000,000		建立區域聯防監系統。	4
	4-1	遠端連線側錄稽核系統(國內自主產品)			1,000,000	資安國內自主產品	9
	4-2	資料加密管理系統(國內自主產品)	管理本府資訊系統機敏資料，以防止個資外洩。		857,000	資安國內自主產品	11
	4-3	資安日誌保存與稽核系統(國內自主產品)	提供資安紀錄分析暨日誌保存機制，以因應資安事件時能快速分析能力。	1,000,000		資安國內自主產品	8
	5	推動ODF為政府文件標準格式		329,000		配合中央政策推動本縣計畫。	5
	6	建立資訊安全管理制度	建立資訊安全管理制度	2,000,000		維護本縣B級機關資安管理制度。	6
	7	行動APP檢	行動APP	600,000		資安國	7

		測認證(國內自主研發)	檢測認證			內自主產品	
	8	系統測試、資料備份			1,000,000	淬煉場域	10
108 年合計				30,286,000			
109 年	1	網路整併費用	汰換網路、資安設備與線路費		20,000,000	汰換基層機關網路設備。	1
	2-1	導入政府組態基準(GCB)，提列以已無原廠維護或無法更新之個人電腦或作業系統(7 年以上)	因不支援新的 GCB 規則個人電腦,伺服器汰換		15,500,000	汰換基層機關本府電腦 100%	2
	2-2	導入 GCB 端點管控機制	導入 GCB 端點管控機制	700,000		導入機關比例 100%	3
	3	建立 SOC 區域聯防監控系統		1,000,000		建立區域聯防監系統。	4
	4-4	原始碼弱點掃瞄管理系統 (國內自主研發)	管理本縣靜態原始碼上線、變更檢測存在弱點。	950,000	1,000,000	資安國內自主產品	9
	4-5	應用系統效能管理工具 (國內自主產品)	本縣重要資訊服務系統效能監控平台		1,929,000	資安國內自主產品	13
	4-6	網路惡意行為與動態分析系統 (國內自主研發)	防範 Web APT 攻擊所帶來之惡意入侵或資料外洩風險。	3,500,000		資安國內自主產品	11
	4-5	郵件防禦與動態分析系統 (國內自主研發)	防範電子郵件 APT 攻擊 APT 與分析未知威脅。	3,500,000		資安國內自主產品	10

	5	推動 ODF 為政府文件標準格式		300,000		配合政策推動	6
	6	建立資訊安全管理制度	建立資訊安全管理制度	2,000,000		維護本縣 B 級機關資安管理制度。	5
	7	APT 巨量資料分析設備(國內自主研發)	APT 巨量資料分析設備	500,000		資安國內自主產品	12
	8	行動 APP 檢測認證(國內自主研發)	行動 APP 檢測認證	500,000		資安國內自主產品	8
	10	系統測試、資料備份			3,000,000	淬煉場域	7
109 年合計				54,379,000			

	四	苗栗縣政府					
108	1	網路整併費用	整併各機關網路	0	10,280,000		1
	2-1	導入政府組態基準，提列以已無原廠維護或無法更新之個人電腦或作業系統(7 年以上)	個人電腦,伺服器汰換	0	8,460,000		2
	2-2	導入 GCB 端點管控機制	導入 GCB 端點管控機制	1,300,000	0		3
	3-1	建立 SOC 區域聯防監控系統		2,028,000	0	建立區域聯防系統。	4
	3-2	成立資安區域聯防中心，與鄰近縣市建立 SOC 資安聯防機制		0	1,016,000	建立緊急應變機制與資安監控機制。	5
	4	意圖威脅即時鑑識機制		0	0		6

	5	資訊安全防護及檢測		0	0		9
	6	APT 巨量資料分析設備		0			8
	7	資料加密管理系統		0	0		7
	8	郵件防禦與動態分析系統		0	0		10
	9	推動 ODF 為政府文件標準格式		0	0	配合推動中央政策。	11
	10	建立資訊安全管理制度		0	0		12
	11	弱點掃描管理系統		0	0		13
	12	系統資料異地備份		0	0		14
108 年合計				23,084,000 元			
109	1	網路整併費用	整併各機關網路	1,000,000	14,782,000		1
	2-1	導入政府組態基準，提列以已無原廠維護或無法更新之個人電腦或作業系統(7 年以上)	個人電腦,伺服器汰換	0	19,472,000		2
	2-2	導入 GCB 端點管控機制	導入 GCB 端點管控機制	1,500,000	0		3
	3-1	建立 SOC 區域聯防監控系統		2,500,000	0	建立區域聯防監系統。	4
	3-2	成立資安區域聯防中心，與鄰近縣市建立 SOC 資安聯防機制		828,000	0	建立緊急應變機制與資安監控機制。	5
	4	意圖威脅即時鑑識機制		2,500,000	0		6

	5	資訊安全防護及檢測		0	0		7
	6	APT 巨量資料分析設備		0	0		8
	7	資料加密管理系統			0		9
	8	郵件防禦與動態分析系統		0	0		10
	9	推動 ODF 為政府文件標準格式		0	0	配合推動中央政策。	11
	10	建立資訊安全管理制度		0	0		12
	11	弱點掃描管理系統		0	0		13
	12	系統資料異地備份		0	0		14
109 年合計				42,582,000 元			
108~109 年合　　計				65,666,000 元			

十、 經費補助表

單位：新臺幣元

機關	年度	總經費	其他基金或補助款	地方政府自籌款(參考 107 年比例)	行政院資通安全處補助款(參考 107 年比例)
桃園市政府	108	131,842,000	0	52,736,800	79,105,200
	109	67,237,000	0	26,894,800	40,342,200
	總計	199,079,000	0	79,631,600	119,447,400

機關	年度	總經費	其他基金或補助款	地方政府自籌款	行政院資通安全處補助款
新竹市政府	108	34,510,000	0	10,353,000	24,157,000
	109	18,775,000	0	5,632,500	13,142,500
	總計	53,285,000	0	15,985,500	37,299,500

機關	年度	總經費	其他基金或補助款	地方政府自籌款	行政院資通安全處補助款
新竹縣政府	108	79,803,000	0	23,940,900	55,862,100
	109	59,025,000	0	17,707,500	41,317,500
	總計	138,828,000	0	41,648,400	97,179,600

機關	年度	總經費	其他基金或補助款	地方政府自籌款	行政院資通安全處補助款
苗栗縣政府	108	90,288,183	0	9,028,818	81,259,365
	109	50,477,468	0	5,047,747	45,429,721
	總計	140,765,651	0	14,076,565	126,689,086

十一、預定進度

查核點是每年 1,4,7,10 月

機關	時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
桃園市政府	108/10	75%	1,690,000	導入政府組態基(GCB)端點管控機制 75%
	109/10	95%	2,190,000	導入政府組態基(GCB)端點管控機制 95%
新竹市政府	108/10	80%	1,972,588	導入政府組態基(GCB)端點管控機制 80%
	109/10	100%	2,472,588	導入政府組態基(GCB)端點管控機制 100%
新竹縣政府	108/10	70%	30,286,000	導入政府組態基(GCB)端點管控機制 70%
	109/10	100%	84,665,000	導入政府組態基(GCB)端點管控機制 100%
苗栗縣政府	108/10	70%	16,158,800	導入政府組態基(GCB)端點管控機制 70%
	109/10	100%	65,666,000	導入政府組態基(GCB)端點管控機制 100%

十二、預期效益

1. 監控維運地方政府資安區域聯防機制，提升地方政府對資安事件之預警與應處能力。

2. 導入政府組態基準(GCB)規範資通訊終端設備（如：個人電腦）的一致性安全設定（如：密碼長度、更新期限等），以降低成為駭客入侵管道，進而減少引發資安事件之疑慮。
3. 強化資安防護設備，減少重大資安事件發生率。
4. 輔導各所屬機關建立資訊安全管理制度及相關規範、開設資通安全專業證照班，以符合資通安全管理法及子法規定。
5. 關鍵系統或重要系統通過源碼檢測，找出應用程式漏洞，避免惡意使用者可輕易的取得機密資訊，強化系統或網站之資通安全。

十三、相關聯絡資料

(含單位、聯絡人姓名、電話、E-mail 等)

項目	機關	聯絡人	電話	E-mail
1	桃園市政府	李清吉	03-3322101#6962	10019015@mail.tycg.gov.tw
2	桃園市政府	黃偉鈞	03-3322101#6961	10037733@mail.tycg.gov.tw
3	苗栗縣政府	歐聰慧	037-559748	jason@ems.miaoli.gov.tw
4	苗栗縣政府	謝明亨	037-559745	herryhsieh@ems.miaoli.gov.tw
5	新竹市政府	林宏叡	03-5216121 分機 340	01024@ems.hccg.gov.tw
6	新竹市政府	莫雅雯	03-5216121 分機 512	010123@ems.hccg.gov.tw
7	新竹縣政府	沈慧虹	03-5518101#3771	hhshen@hchg.gov.tw
8	新竹縣政府	許添財	03-5518101#3771	Hsu_Tien_Tsai@hchg.gov.tw

附表 1: 網路整併費用

1. 桃園市政府

年別	項次	名稱	規格	數量	單位	單價	總價	備註
108	1	網路流量導流設備		1	台	1,977,000	1,977,000	配合整併案本府須購置設備
	2	網路交換器	JUNIPER EX3300-24T-TAA	12	台	67,500	810,000	
	3	防火牆	FG-501E（含三年特徵碼更新）	12	台	650,000	7,800,000	每公所 2 台 HA 架構
	4	服務人力費用	區公所人力建置費用 6	6	點	71,830	431,000	經常門
		資本門小計	第 1+2+3 項				10,587,000	
		經常門小計	第 4 項				431,000	
		合計					11,018,000	

年別	項次	名稱	規格	數量	單位	單價	總價	備註
109	1	網路交換器	JUNIPER EX3300-24T-TAA	14	台	67,500	945,000	
	2	防火牆	FG-501E（含三年特徵碼更新）	14	台	650,000	9,100,000	每公所 2 台 HA 架構
	3	服務人力費用	區公所人力建置費用 7	7	點	72,000	504,000	經常門
		資本門小計	第 1+2 項				10,045,000	
		經常門小計	第 3 項				504,000	
		合計					10,549,000	

2. 新竹市政府

項次	項目	單位	單價	108 年		109 年	
				數量	金額	數量	金額
1	網路服務人力	人月	69000	11	759,000	11	759,000
2	USER 端安全防護	台	3800	350	1,330,000	650	2,470,000
3	負載平衡器	台	1,250,000			2	2,500,000

4	IPS	台	1,900,000	1	1,900,000		
5	CoreSwitch	台	400,000	1	400,000		
6	L3 Switch	台	45,000	8	360,000	4	180,000
7	L2 Switch	台	17,500	28	490,000	15	262,500
8	網路附加儲存系統 NAS	台	100,000	2	200,000		
9	DNS Server	台	150,000	3	450,000	1	
10	網路設備主機	台	195,500			5	977,500
	小計				5,889,000		7,149,000
	總計	13,038,000					

3. 新竹縣政府

項次	項目	單位	單價	108 年		109 年	
				數量	金額	數量	金額
1	整併線路後，更換本縣公務機關網路與資安設備	式	5,000,000	1	5,000,000	2	10,000,000
2	防火牆日誌收集及分析伺服器	式	2,000,000			1	2,000,000
3	汰換網路名稱解析伺服器	式	3,000,000			1	3,000,000
4	汰換 Web 安全閘道服務系統	式	5,000,000			1	5,000,000
	小計				5,000,000		20,000,000
	總計	25,000,000					

4. 苗栗縣政府

項次	項目	單位	單價	108 年		109 年	
				數量	金額	數量	金額
1	VPN 網路建置	式	1,000,000	1	1,000,000	0	0
2	區域聯防設備	台	210,000	18	3,780,000	18	3,780,000
3	區域聯防設備整合管理設備	台	1,000,000	0	0	1	1,000,000
4	網路智能管理設備	式	4,000,000	0	0	1	4,000,000
5	IP/MAC 控管暨端點防護	式	2,000,000	0	0	1	2,000,000
6	資產管理軟體	式	3,002,000	0	0	1	3,002,000
7	防火牆 APT 設備	式	4,700,000	0	0	0	0
8	網路負載平衡設備	台	1,000,000	0	0	1	1,000,000
9	意圖威脅即時鑑識機制	式	5,500,000	1	5,500,000	0	0
	小計				10,280,000		14,782,000
	總計	25,062,000					

附表 2: 為能順利導入政府組態基準(GCB)，提列以已無原廠維護或無法更新之個人電腦或作業系統(7 年以上)

1. 桃園市政府

項次	項目	單位	單價	108 年		109 年	
				數量	金額	數量	金額
1	個人電腦	台	41, 000	880	36,080,000	690	28,288,000
	總計						64, 368, 000

2. 新竹市政府

項次	項目	單位	單價	108 年		109 年	
				數量	金額	數量	金額
1	個人電腦	台	35,000	120	4,200,000	61	2,135,000
2	伺服器(中階)	台	200,000	5	1,000,000	5	1,000,000
	小計				5,200,000		3,135,000
	總計						8,335,000

3. 新竹縣政府

項次	項目	單位	單價	108 年		109 年	
				數量	金額	數量	金額
1	個人電腦(螢幕)	台	25,000	400	9,903,000	369	9,225,000
2	資訊系統、網路設備測試環境	式	5,000,000	1	5,000,000		
3	資訊系統、網路設備測試環境(擴充)	式	2,500,000			1	2,500,000
4	汰換基層機關資訊系統伺服器	式	3,000,000	1	3,000,000		
5	汰換本府資訊系統伺服器	式	3,000,000	1	3,000,000	1	3,000,000
	小計				20,903,000		14,725,000
	總計		35,628,000				

4. 苗栗縣政府

項次	項目	單位	單價	108 年		109 年	
				數量	金額	數量	金額
1	個人電腦	台	35,000	1,278	44,730,000	224	7,840,000
2	筆記型電腦	台	38,000	12	456,000	9	342,000

3	伺服器(高階)	台	415,000	20	8,300,000	19	7,885,000
4	伺服器(中階)	台	218,000	40	8,720,000	37	8,066,000
5	防火牆(中階)	台	1,000,000	1	1,000,000	0	0
6	防火牆(中低階)	台	600,000	1	600,000	3	1,800,000
7	防火牆(低階)	台	200,000	9	1,800,000	1	200,000
8	CoreSwitch	台	1,800,000	1	1,800,000	1	1,800,000
9	Layer3 Switch	台	150,000	17	2,550,000	6	900,000
10	Layer2 Switch	台	40,000	14	560,000	1	40,000
	小計				70,516,000		28,873,000
	總計	99,389,000					

附件 6

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之分項計畫

臺中市

108年3月

臺中市政府
強化政府基層機關資安防護及中彰投區域聯防計畫

一、計畫緣起

自民國 80 年政府推動行政電子化以來，已經有效提升本國行政效能，尤其各項為民服務評比，都必須借重資訊科技以提供創新服務，最有名的莫過於李總統登輝先生推動的跨區辦理戶籍異動，而近年來，網路報稅更顯得簡便，各種跡象顯示，行政作業使用資通訊的應用越來越多，衍生出資安問題也日益嚴重，經過行政院資通安全處調查，全國資安專職人力約缺少 1 千多人，臺中市政府調查各機關辦理資安責任等級應辦事項所需預算金額需增列 2 千 1 百多萬元，其他基層機關則更缺乏預算，而無法達成政府機關(構)資通安全責任等級分級作業規定。

因應行政院 106 年 4 月 5 日核定通過之「前瞻基礎建設計畫」，其中「數位建設」子項目-「強化政府基層機關資安防護及區域聯防」須提出競爭型計畫以爭取中央補助，並考量地方政府基層機關經費及人力不足，資安防護薄弱，確有加強資安區域聯防之必要。臺中市政府爰結合彰化縣、南投縣等鄰近區域縣市政府及產學界共同提案以強化基層機關之資安防護以符合行政院函頒之「政府機關(構)資通安全責任等級分級作業規定」強化基層資安防護、提升基層機關之資訊服務能量、建置區域資安聯防、加強資安防禦縱深及創新服務整合及持續營運規劃，亦期能有助於帶動國內資安產業發展，特擬訂本計畫。

二、 計畫目標

本案經考量基層電腦老舊、資訊人員匱乏等情形，運用本國自有資訊安全產品及服務，整合產官學能量，規劃中彰投區域資安聯防機

制，並期能在計畫結束後，整合機關及學術之資安人力，建立中彰投資安快速應變小組，並完成下列目標。

(一) 汰換老舊資訊軟硬體設備

(二) 內部風險及威脅管控

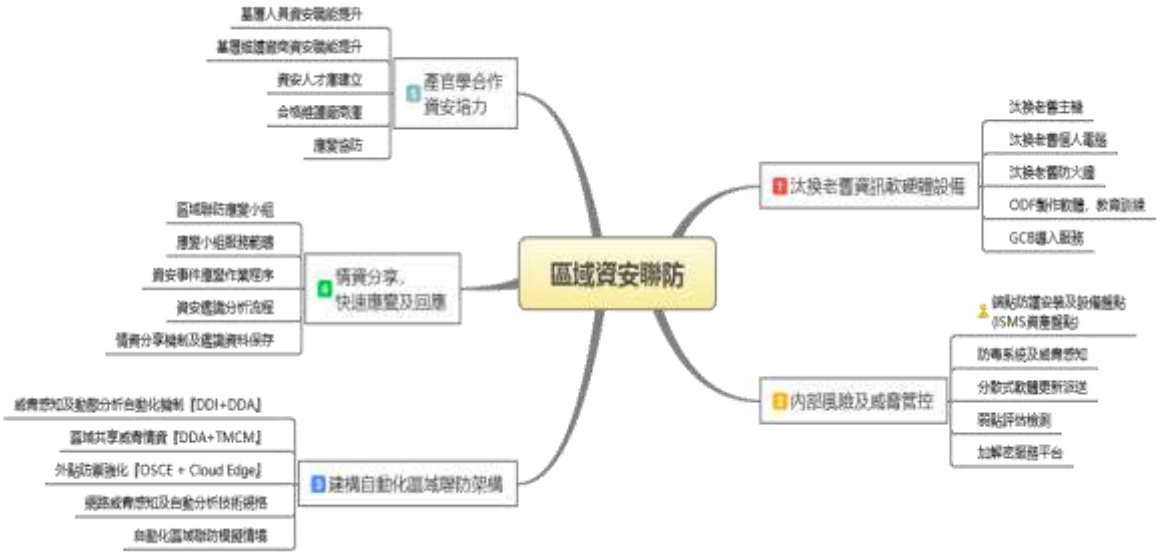
(三) 建構自動化區域聯防架構

(四) 情資分享，快速應變及回應

(五) 產官學合作資安培力

三、 計畫內容與實施策略

以下就五大項計畫目標分別補充說明其工作內容，主要的解決方案，市場上已經有相對應產品，考量計畫時效，優先採用共同供應契約之資安服務項目。



(一) 汰換老舊資訊軟硬體設備

1、 汰換老舊主機、個人電腦及防火牆等軟硬體：

本次經調查彰化縣及南投縣政府及鄉鎮市公所，發現有許

多機關仍使用 XP 版本電腦，因此無法進一步經由組態設定或是系統更新以確保其安全性，主機伺服器及防火牆等也有類似情形，部分鄉鎮市公所甚至未具備防火牆，後續則依調查老舊設備的結果或是缺乏基本防火牆設備，這些設備已無原廠維護或無法更新之個人電腦或作業系統，不能經由修補以提升自我防護能力，爰彙整數量金額以爭取補助。

臺中市政府自 103 年起協助所屬機關進行電腦汰換作業，累計已經超過 6,000 台以上，現行多數電腦尚未達使用年限，且 Windows 7(民國 99 年以後購置之電腦)作業系統已符合基本資安要求，政府經費有限，本次專案則以汰換剩餘老舊 XP 電腦為目標，可以節省大量的經費，並提昇最後一哩端末設備的安全性。

2、ODF 製作軟體及 GCB 政府組態基準導入：

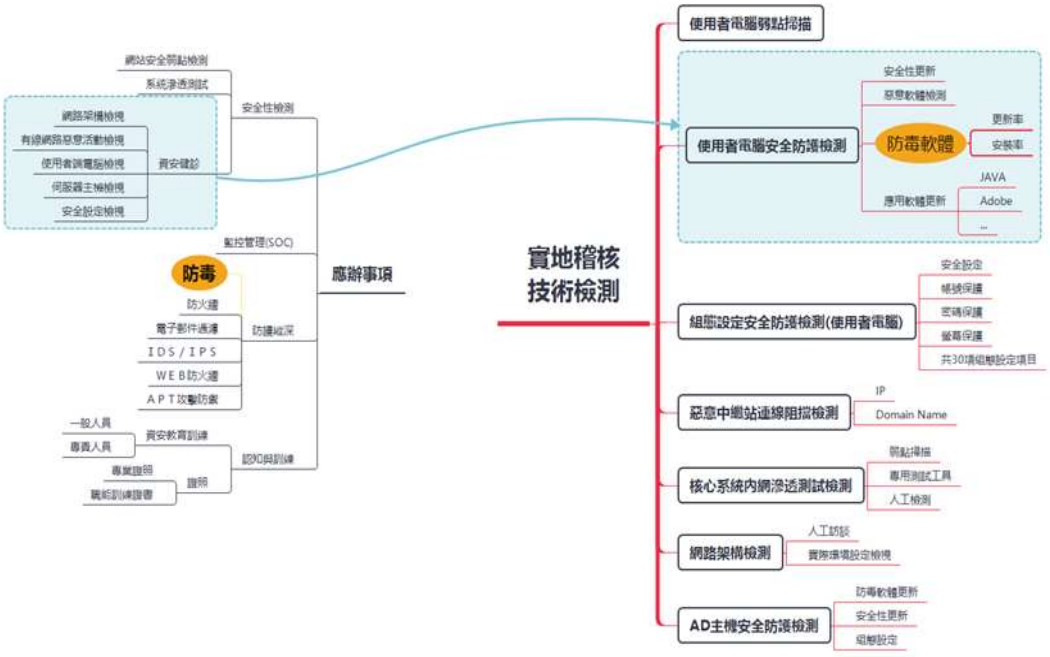
汰換電腦作業同時會要求廠商安裝 ODF 製作軟體，以推廣開放資料格式，並設定政府組態基準 GCB，導入一致性安全設定(如：密碼長度、更新期限等)，以降低成為駭客入侵管道，進而引發資安事件之疑慮。

(二) 內部風險及威脅管控

根據趨勢科技公司統計，臺灣企業平均遭駭客入侵潛伏的時間長達 598 天，甚至發現有高科技公司遭駭客入侵了 11 年而無人發現，資安防護思維必須改變。國際知名的調研組織 Gartner，早在 2014 就提出「預防無用論」 (Perfect prevention is impossible) 的概念，強調組織應永遠假設自身正在遭受駭客的攻擊入侵，企業得先意識到自己「必定遭駭」來規劃全然不同思維的資安防護措施，防禦的對象也從外部，轉而增加內

部的防禦，強化威脅情資的蒐集，進而縮短發現入侵點及時間，以有效應變及控制損失，這也是資安領域專家的共同共識。

資訊安全管理是一種風險管理的概念，行政院為提升政府機關整體資安防護能力，經參考 102 年網路攻防演練及政府機關(構)資安健診、稽核結果，採納國際資訊科技發展及資通安全威脅趨勢，針對各政府機關(構)所面臨共通問題，規劃資安防護強化措施，依政策、管理、技術及認知與訓練之四個面向，檢討修訂資安責任等級應辦事項，其中「安全性檢測」項目就是一種風險的評估方式，用以找出漏洞所在，提醒機關注意修補以免遭受入侵。



另外，行政院國家資通安全會報為協助各機關強化資通安全(以下簡稱資安)防護工作之完整性及有效性，並透過持續改善以降低資安風險，於網際防護體系下設「稽核服務組」；並依「國家資通訊安全發展方案(102 年至 105 年)」行動方案 2.3.3

「落實資安稽核作業」，每年至少選定 20 個重要機關辦理資安外部稽核，並彙整稽核缺失資料。

臺中市政府將應辦事項內容及實地稽核之技術檢測項目內容，採用文字雲的方式分析及呈現，發現「使用者電腦」、「防毒軟體」及「安全性更新」這幾個詞彙占比最高，為此，防毒系統及威脅感知、弱點評估檢測、軟體更新派送及資產盤點等 4 個工作應優先納入內部風險及威脅管控項下。

1、 端點程式安裝及設備盤點：

曾經推動過資訊安全管理制度的人都知道，管理的第一步就是要資產盤點以產製資產清冊，這份清冊並不是財產的清冊，不是可以從財產系統產出來的。以臺中市政府、彰化縣政府及南投縣政府而言，這些應該都是已經完成的工作，透過本次調查，發現許多基層公所連防毒系統都沒有，如前所述，防毒是最基本也是最重要的防護要求，後續亦規劃納入弱點評估及軟體更新派送等資安機制並考量基層公所既沒有導入資訊安全管理制度，也沒有資訊人員，在此規劃由資訊業者提供安裝檢測服務，並進行設備盤點。

2、 防毒系統及威脅感知：

對多數人來說，防毒就是找到一套可靠的防毒軟體安裝到電腦或是主機系統，這麼一件簡單的事，如果防毒程式發現病毒、蠕蟲及木馬等具威脅的程式，就發揮作用將之移除，不過，臺中市政府卻很慎重地把它當成一件資安「威脅」情資，同樣的情形，大陸國家級資安組織(CNCERT/CC)也把防毒當成一件重要的事，並且每個月都發布感染病毒數量統計報告，就下圖所示，感染病毒的狀態，甚至與網站被入侵的狀態同等重要。

臺中市政府共構網路共收容有 1 萬 6 千個使用者，為有效了解實際中毒狀況，客製一套即時報表系統，這套系統經由市府機關同仁授權帳號，就可以自行透過網頁了解自身機關內的病毒感染情形，加上市府資訊安全長的重視，很快的感染病毒數量迅速減少，管理機關甚至可以經由系統內建規則找出經常性中毒的電腦及使用者，予以通報警示，以降低內部的風險，資訊公開透明，造成同儕之間的

壓力，促使大家遵守網路倫理規範，這也是這套系統最大的效用。

上述機關防毒報表系統將提供本計畫參與縣市，作為共通平台，參與機關可以購買授權後使用。

3、分散式軟體更新派送：

基於以下理由，機關有必要建置軟體更新派送功能，第一，因應行政院資通安全會報辦理資安稽核，主機及個人電腦之安全防護檢測必定會進行包含防毒軟體、安全性修補程式更新、惡意程式防護、JAVA 與 Adobe 應用程式更新等 4 項安全防護措施檢測，使用軟體更新派送系統，是一種簡單有效、節省人力而容易達標的方法。其次，因業務需求，需要將程式或是組態設定等，在短期內安裝派送到所有電腦內，例如：曾經發現一種勒索病毒會在特定目錄寫入一個專屬檔案，這時候就可以運用這樣的機制，模擬已經中毒情形，病毒就不致感染。

以臺中市政府擁有 1 萬 6 千個終端設備來說，大型檔案的派送將占用大量的頻寬，甚至影響到公務作業，而增

加頻寬，除線路費用增加以外，相關的網路設施也都必須配合更換更高等級的產品，綜合以上，預算將呈現倍數增長，一個分散式軟體派送系統是一種非常適合的解決方案。

當偵測或是發現威脅時，軟體更新派送就可以派上用場，例如：最近的想哭(WannaCry)勒索病毒大量感染，運用這樣的機制可以快速完成大量派送，也可以很快降低威脅所造成的損失。

另一個案例是發現免費軟體內被植入類似木馬程式，有主動對外連線行為，可是數量眾多，使用軟體更新派送程式也可以協助一併移除類似的威脅，降低使用人力。

4、弱點評估檢測：

行政院訂定的政府機關(構)資通安全責任等級應辦事項也要求定期對於網站進行安全檢測，重要系統滲透測試，對於個人電腦及網路進行資安健診，目的在於找出弱點所在，前亦引述 2014 年提出的「預防無用論」 (Perfect prevention is impossible)，其目的是要管理者不要一昧的購買防禦性產品，應該了解風險及組織弱點所在，駭客基本上必須利用弱點才能有效入侵到組織內部，人員弱點部分，基本上是透過社交工程提高其警覺性，而系統及設備的種類及數量眾多，透過共用弱點掃描檢測平台，使各級機關能有效掌握本身聯外服務之設備是否存在弱點，並能有效自主管理，設定排程進行掃瞄，減少人力介入。

5、加解密服務平台

相較於 HTTP，HTTPS 是可保護傳輸內容較安全的網

路通訊協定，可防止資料遭竊或竄改。蘋果公司也開始要求 iOS app 開發者應於 2016 年底前全面採用 HTTPS 協定，Facebook 的新聞推播（Instant Article）也是透過 HTTPS 傳送，Google 宣布自 2017 年 1 月起，當 Chrome 使用者瀏覽到低安全性的 HTTP 網站時，網址列將出現「不安全」的警告標示，提醒用戶資料可能因此遭竊。

在強調加密保護的同時，駭客已進化，運用這樣的防護衣，遠端控制設備，並在內網活動或加密打包隱藏，導致現有資安設備失去功能，無法有效防堵。

目前，Chrome 的網頁流量已有超過一半來自 HTTPS，隨著各家科技大廠紛紛優先使用 HTTPS，也意味著 HTTP 終將消失。因此，導入加密訊息解密(SSL/TLS Offloading)服務平台，可減輕現有網管設備(F/W, IPS)的負擔，並提高資安設備分析的效能，將封包解密後的資料，送給資安設備判讀，有助於蒐集威脅情資，進行防禦，本計畫參考教育部區網中心的作法，爭取前瞻計畫補助購置相關軟硬體設施，以提升整體資安防禦效能。

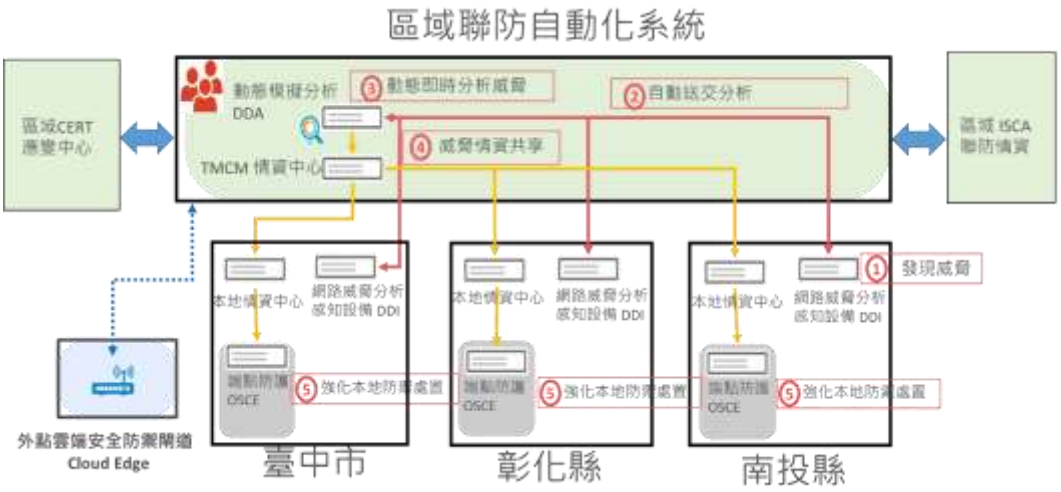
(三) 建構自動化區域聯防架構

基於區域聯防的跨地理特性、與外點單位的防禦機制落差實際狀況，在架構設計上考慮「多地聯合防禦機制」的建立，兼併解決基層資安人力不足問題，因此區域聯防架構設計，採以技術自動化方案，引進國內資安業者之專家型系統，形成一組自動化資安區域聯防堡壘。

在自動化區域聯防架構中，除了各縣市政府既有的資安設施及網路環境外，需要建置一處跨縣市提供彙整資訊與威脅分

析的區域聯防中心。區域聯防中心可以實體建置在區域中的任一個縣市的既有資訊環境內，統一由此一縣市執行威脅分析與事件管理。若考量行政管理權責、與機敏資料保密維護等因素，也可以導入虛擬區域聯防中心的概念，透過雲端運算的技術，委由擁有資安專業服務能力的第三方執行。

整體區域聯防自動化系統架構如下圖：



上方示意圖區域聯防中心在三縣市以外，以虛擬區域聯防中心的架構來呈現整體規劃概念。在這個架構下，標準化區域聯防的工作流程： 威脅即時發現→ 資訊自動送交分析→ 執行動態威脅分析工作→ 跨地提供情資共享→ 強化本地防禦能力。當防禦流程被有效串聯，整個區域就可以一次一次的反複流程中，達到自我增益防護能力的目標。本項自動分析威脅攻擊與下一節「情資分享，快速應變及回應」，本是相輔相成、彼此加乘的機制。當威脅情資可以跨區分享，將彙整大量的威脅資訊，透過大數據運算技術進行分析。

以下就自動化區域聯防之服務及部署方式加以說明：

1、 威脅感知及動態分析自動化機制『DDI+DDA』

本規劃項目主要以區域聯防之縣市政府為主，在縣市政府建立區域內整體網路威脅感知單元(Deep Discovery Inspector, 簡稱 DDI)，區域聯防中心建置共享威脅攻擊樣本自動分析(Deep Discovery Analyzer, 簡稱 DDA)機制。當有威脅鎖定本區域攻擊時可即時被偵測防護且將可疑威脅樣本自動送交動態模擬分析設備，即時進行程式的動態模擬分析，並產出相關威脅情資，達到威脅即時的偵測，樣本自動分析的效用，可以大幅減省採樣鑑識的時間及資安人力的介入。

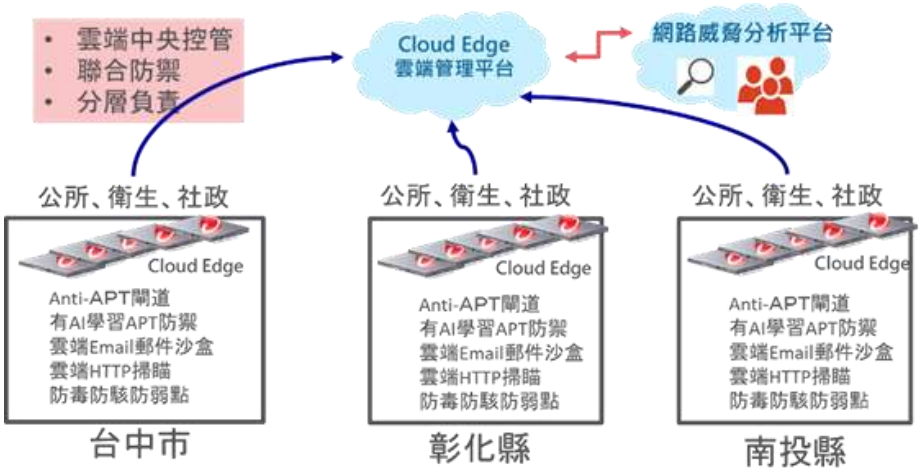
2、 區域共享威脅情資『DDA+TMCM』

區域聯防中心必須發揮「提高攻擊或威脅存在的可見度(Visibility)」最大的優勢，這一點對於具有高度潛伏與隱匿特性的目標式攻擊特別重要，因此，自動化區域聯防的機制在於收到動態威脅分析情資後，可自動回饋同步到各縣市政府的情資中心(TrendMicro Control Manager, 簡稱 TMCM)，達到威脅情資共享的效用，自動化情資分享整體運作在網路順暢情形下，自收到樣本、進行分析、產出情資，可在 30 分鐘內完成共享威脅情資作業。

3、 外點防禦強化『OSCE + Cloud Edge』

在縣市政府的各區域的情資中心取得共享威脅情資後，便可以將威脅情資及防禦機制派送到網路威脅偵測感知單元及轄下所有管理中的端點安全防護機制(OfficeScan Corporate Edition, 簡稱 OSCE)，以達到整體全面性的防禦強化。

考量彰化縣及南投縣仍有許多的外點單位,如警察、消防、衛生、環保、稅務及鄉鎮市公所等，這些單位具備許多資訊終端設備，且各自資訊安全管理的能量可能存在落差。因應這樣的實際情況，為了在可分層負責的架構下，擁有區域聯防的資源共享優勢，就必須考量雲端中央管理的做法。



本項規劃主要強化基層鄉鎮市公所或府外機關使具有一致性防禦能力，運用端點防護(OSCE)及網路閘道功能(Cloud Edge)，並加入整體區域聯防機制內，一方面可用以監控內、外部威脅，回饋可疑威脅來源到區域聯防中心，又可以一併接受共享情資進行防禦，將比現有防火牆及入侵偵測系統，更能有效處理多變的攻擊行為，既可達到阻止入侵及內部擴散的目地，亦可解決基層資安人力不足問題。

4、 網路威脅感知及自動分析技術規格

- 網路威脅感知單元(DDI)

用來分析區域內網路包含網頁，郵件...超過 100 種網路協

定與應用程式行為。且依各區域需求分析內網到外網、內網到內網與重點主機網路流量進行整體分析一旦發現有可疑網路活動行為的存在，能更精準定位潛伏在內部的感染源，此防禦機制的好處是可以偵測 APT 威脅行為，感知並定位威脅的存在，支援網路設備阻斷與外部有害的 C&C 連線，並可自動將惡意樣本送交 DDA 動態模擬分析。

(1) 網路威脅偵測設備，對 OSI 7 Layers 的第 2-7 層協定進行掃描。
(2) 支援超過 100 種網路協定及應用內容分析。
(3) 有效偵測中繼站 C&C 連線事件，定位威脅控制之電腦。
(4) 套用 APT 專屬規則，對內網進行過濾，定位受駭電腦。
(5) 偵測高風險檔案威脅，並主動提交 DDA 進行動態威脅分析。
(6) 接受回饋之分析結果，主動加入惡意連線偵測清單。

- 動態威脅模擬分析(DDA)

在經過閘道端 DDI 網路威脅分析的偵測攔截後，可以分離出有害與可疑程式，並將可疑程式樣本後送至 DDA 動態分析平台，進行動態威脅模擬分析。

這是區域聯防自動化的第二道關卡，可以即時分析出針對性的區域專屬攻擊威脅，擷取惡意攻擊行為中相關的惡意程式樣本，動態分析取得 C&C、IP、FQDN、Sha1 等等威脅情資，提供給回饋式整體循環防護做為依據。對於區域聯防系統可以提供即時的情資更新與學習，立即強化防禦能力效用。此自動化防禦機制的好處是可以進行自我學習，

除了強化自身防禦能力外，並提供聯防情資中心製作專屬解藥的必要資訊。

(1) 沙箱分析設備，具備多個動態威脅分析器。
(2) 驅動樣本行為重演，並針對惡意行為和對系統影響做深度追蹤。
(3) 可自動接受多種產品自動提交樣本(DDI、OSCE、IMSVA)，或是手動上傳可疑檔案。
(4) 判別惡意的C&C 中繼站位址，自動回饋設備進行本地端防護。
(5) 可匯入 STIX 威脅情資，進行樣本動態分析。
(6) 提供惡意威脅的執行和評估摘要報告。
(7) 可匯出樣本檔案提交病毒碼製作。

5、 自動化區域聯防模擬情境

以自動化區域聯防的架構來呈現整體規劃概念，當防禦流程被有效串聯，整個區域就可以在一次一次的反複流程中，達到自我增益防護能力的目標。本項自動分析威脅攻擊與共享威脅情資，可相輔相成、彼此加乘的機制。當威脅情資可以跨區分享，將彙整大量的威脅資訊，透過大數據運算技術進行分析。以下列出本計畫採用設備及服務流程模擬情境：

[情境一]：當區域內網路感知攻擊威脅，自動啟動動態威脅分析，即時將威脅情資共享及防禦套用。

在這個架構下，標準化區域聯防的工作流程如下：

(1) 各地區域網路威脅設備 DDI 發現攻擊威脅，自動送交

聯防中心的動態威脅分析設備 DDA。

(2) DDA 執行動態威脅分析工作且產出威脅情資(Sha1、IP、URL、Domain)。

(3) 聯防情資中心 TMCM 共享威脅情資給各縣市政府情資中心。

(4) 各縣市的情資中心派送威脅情資給本地的網路威脅設備 DDI 及端點安全防護軟體 OSCE，強化本地防禦能力。

[情境二]：區域內部各地(縣市)資安管理員，採集到可疑攻擊程式或者可疑網址，手動送交動態威脅分析，可即時將威脅情資共享及防禦套用。

(1) 各縣市政府資安管理單位，採集可疑攻擊程式或者可疑網址，手動送交聯防中心的動態威脅分析設備 DDA。

(2) DDA 執行動態威脅分析工作且產出威脅情資。

(3) 聯防情資中心 TMCM 共享威脅情資給各縣市政府情資中心。

(4) 各縣市政府情資中心派送威脅情資給本地的網路威脅設備 DDI 及端點安全防護軟體 OSCE，強化本地防禦能力。

[情境三]：區域內部端點電腦安全防護軟體 OSCE，偵測可疑未知檔案，自動送交動態威脅分析，可即時將威脅情資共享及防禦套用。

(1) 區域內部端點電腦安全防護軟體 OSCE，偵測可疑未知檔案(來自網頁、郵件下載、USB)，自動送交聯防中心的動態威脅分析設備 DDA。

(2) DDA 執行動態威脅分析工作且產出威脅情資。

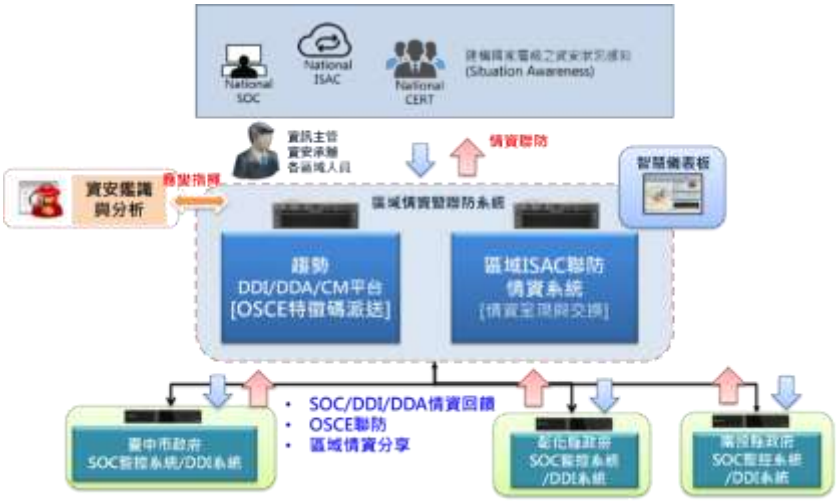
(3) 聯防情資中心 TMCM 共享威脅情資給各縣市政府情資中心。

(4) 各縣市政府情資中心派送威脅情資給本地的網路威脅設備 DDI 及端點安全防護軟體 OSCE，強化本地防禦能力。

(四) 情資分享，快速應變及回應

情資分享主要工作為建立分享與收集內外部資安情資(如惡意中繼站(DN/IP))與攻擊活動訊息(如可疑郵件主旨列表、可疑連線 IP、惡意留言等)，如有發現大規模之網路攻擊(如勒索軟體、蠕蟲發作等)時，即時通知所屬本案區域縣市(臺中市、南投縣、彰化縣)之資安駐點人力並透過 DDI/DDA/TMCM 平台進行預防或增設偵測/阻擋規則。

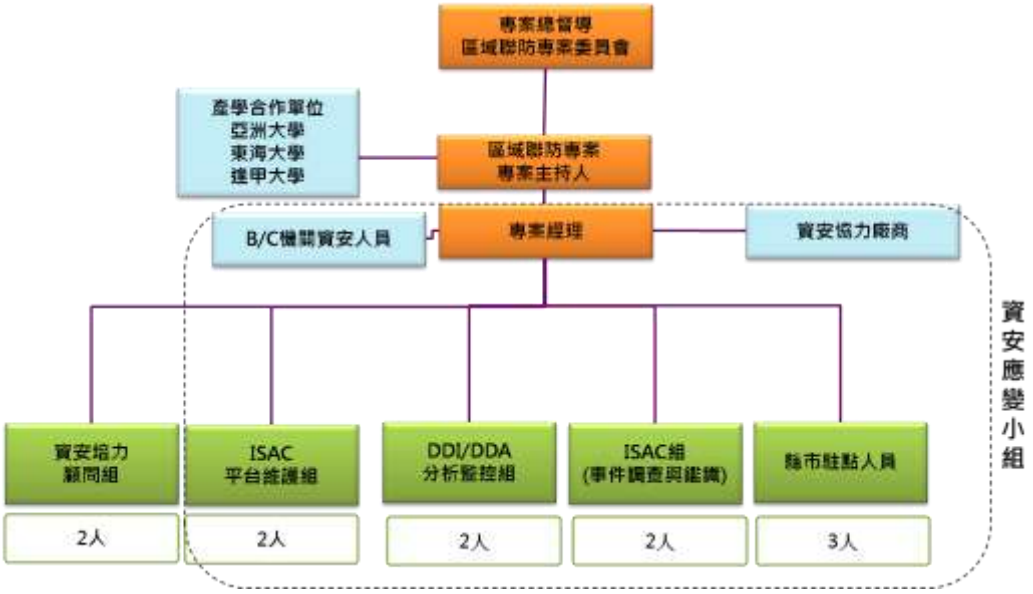
監測發現聯防範圍內之資安事件，一線資安人員應於第一時間辨別其影響範圍及風險等級外，另外須透過資安應變小組的機制，提供所屬鄰近縣市之資安協防、技術支援；除此之外，應變小組需負責日常資訊分享與分析中心(ISAC)維運、資安情資交換運作及派送阻擋規則，同時可對應各級機關資安人員建立三級資安風險應變制度及提供專家顧問諮詢服務。



圖：中彰投區域情資暨趨勢聯防系統服務架構

1、 區域聯防應變小組

臺中市政府將協同彰化縣政府及南投縣政府成立「中彰投資安區域聯防委員會」，以協調、整合及督導資安區域聯防工作，其組成包括區域聯防資安專案服務廠商(含四個分組，分別是 ISAC 平台維護組、DDI/DDA/TMCM 管理維運組、ISAC 組與縣市駐點人員組、資安培力顧問組)、資安協力廠商及縣市政府資安專責人員等，並以虛擬化組織成立「中彰投資安應變小組(以下簡稱 TCN CERT)」以協防及即時回應所屬鄰近縣市事件通報單位(臺中市、彰化縣、南投縣，以下簡稱 CI/Confidential Informants 提供者)在重大資安事件發生後執行緊急應變、入侵管道定位、受影響範圍評估及應變受駭系統，提供處置改善建議，並與產學合作單位協同研議流程規劃及後續改善與後續案例宣導教育訓練，參考技服中心「領域 CERT 實務建置指引」及美國國家標準與技術研究院(NIST)的「Computer Security Incident Handling Guide (SP800-61r2)」建立事件故處理流程及依據「國家資通安全通報應變作業綱要」處理流程進行通報回應。



圖：區域聯防專案組織暨資安應變小組（TCN CERT）組織架構圖

(1) 各分組職能說明如下:

A. 【ISAC 平台維護組】

- 日常維運時:負責 ISAC 平台維護、情資發布、資安事件故通報、使用 ISAC 平台設定防護規則阻擋新惡意中繼站。

B. 【DDA/DDI/TMCM 管理維運組】

- 日常維運時：負責回饋及分享縣市機關 DDI 資安情資與管理。
- 發生資安事件故時:結合各縣市駐點人力，現場支援協助資安事件故之前置作業與資料蒐集，合力進行資安事件故分析處理。
- 發生資安事件故時：針對 3 線所分析後的惡意情資來源使用 DDI/DDA/TMCM 平台設發布 OfficeScan 防護特徵值。

C. 【ISAC 組(事件調查與鑑識)(3 線) 】

- 日常維運時：負責規劃資安應變程序及情

資咨詢。

- 發生資安事件故時：資安事件應變程序指揮與判斷。

D. 【縣市駐點人員(1 線)】

- 日常維運時：負責聯防設備規則調校與資安事件/故確認。
- 發生資安事件/故時：現場支援協助資安事件/故之前置作業與資料蒐集。

E. 【資安協力廠商(2 線)】

- 發生資安事件/故時：現有資安協力廠商(如：一線 SOC 資安廠商、資安設備維運廠商、系統服務廠商)，則應配合協助處置。

F. 【縣市政府資安專責人員】

- 發生資安事件/故時：配合輪值指揮官，協調機關內部人員及現有資安協力廠商(如：一線 SOC 資安廠商、資安設備維運廠商、系統服務廠商)協助處置，並辦理通報、支援需求等行政作業。

G. 【資安培力顧問組】

- 負責協助推對區域內產學合作資安培力計畫與執行，負責擔任及安排課程講師顧問及執行秘書任務人員。

2、 中彰投資安應變小組(TCN CERT)服務範疇

本次規劃區域 CERT 功能包括事件通報管理、事件處理分析、技術支援與協助及教育訓練等。

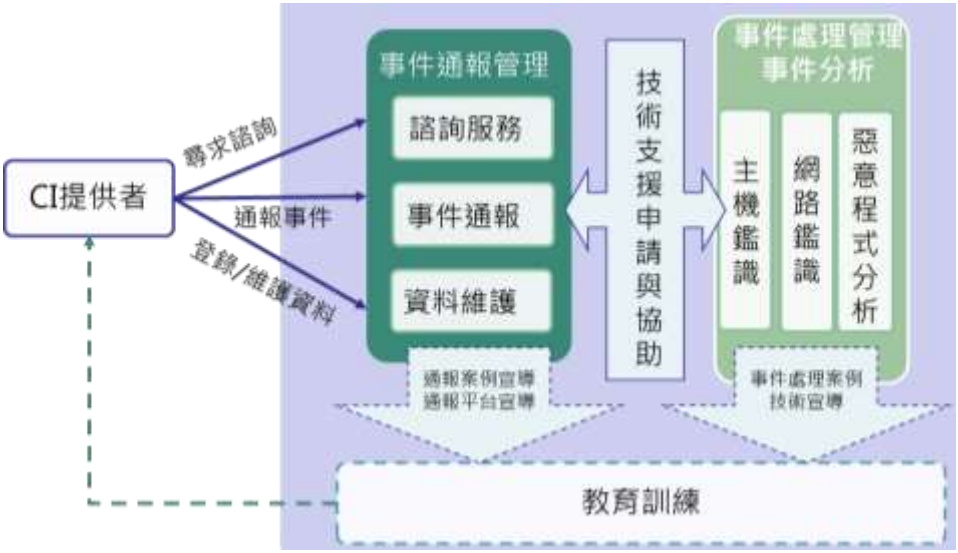


圖:TCN CERT 維運模式說明
(資料參考:技服中心 領域 CERT 實務建置指引)

應辦事項詳如下列說明：

應辦事項	說明
建立資安事件通報程序	CI 提供者發生資安事件時，須向 TCN CERT 窗口進行通報。事件等級建議詳見國家資通安全通報應變作業綱要等級劃分原則，依「機密性」、「完整性」及「可用性」由輕至重分為 1 至 4 級資安事件。若該筆資安事件為 3、4 級資安事件，領域 CERT 須逐層上報至國家層級 N-CERT。
建立資安事件處理程序	CI 提供者發生資安事件時，若需請求外部技術支援，TCN CERT 得視需求提供事件處理協助。若該筆資安事件為 3、4 級資安事件，且需外部協助時得向國家層級 N-CERT 申請支援。
CI 提供者資料維護管理	提供管道供 CI 提供者進行資料維護與更新。
維護資安事件通報平台	協助管理資安事件通報、事件處理及 CI 提供者資料維護。

資料參考:技服中心領域 CERT 實務建置指引

3、資安事件應變作業程序

TCN CERT 將整合【區域聯防專案委員會】下轄各分組任務編組外，並結合縣市政府機關(A、B、C、D 級機關)資安人員及現有資安協力廠商(如：一線 SOC 資安廠商、資安設備維運廠商、系統服務廠商)形成虛擬團隊，透過區域聯防機制及地利之便，在重大資安事件發生後立即啟動緊急應變，發動應變流程如下。

圖:資安事件通報暨應變流程說明

如遇「國家資通安全通報應變作業綱要」之「4」、「3」級事件(故)如:惡意(程式、網路)攻擊、非經授權之存取、資料遭竄改或竊取、資訊服務遭攻擊中斷服務病毒蠕蟲爆發之高風險事件。將於事件(故)通報或事件(故)發生 60 分鐘內依據 CI 提供者需求採電話、傳真、手機簡訊、電子郵件等方式，將資訊安全事件(故)通報本機關（構）資訊安全事件聯絡人員，並立即協助事故的後續處理作業並依據事件嚴重性通報 N-CERT，整體三級資安事件通報流程說明如下

CI 提供者	TCN CERT	N-CERT

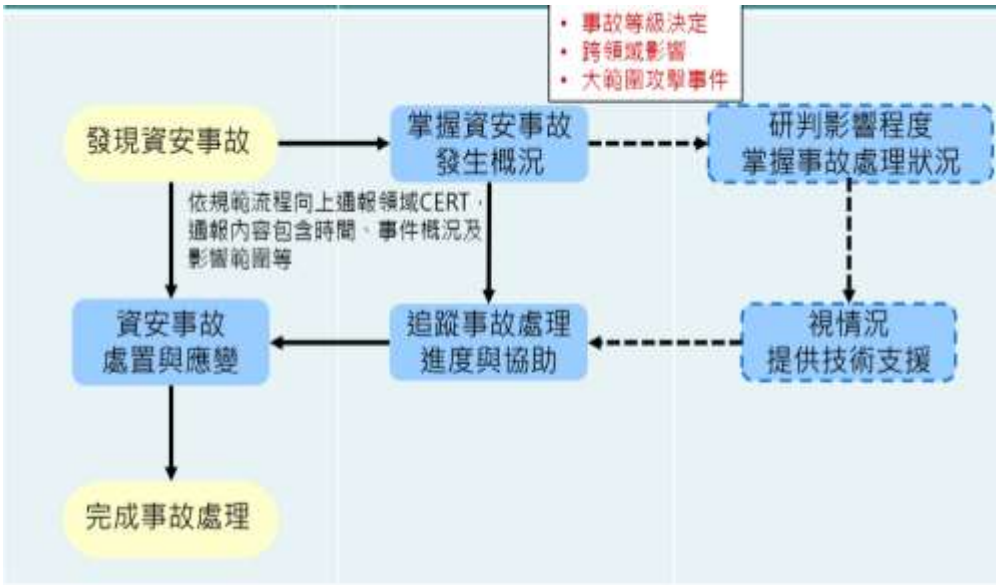
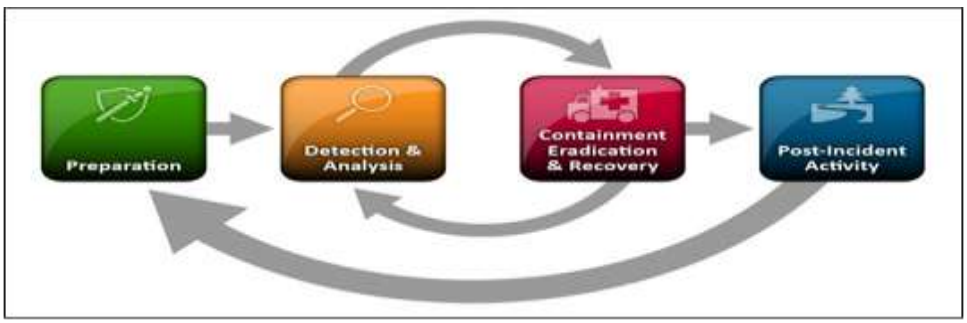


圖: 資安事件通報流程示意圖

(資料參考:技服中心 領域 CERT 實務建置指引)

4、 資安鑑識分析流程說明

執行方式：本機關將參考美國國家標準與技術研究院(NIST) 的【Computer Security Incident Handling Guide (SP800-61r2)】建立事件故處理流程，共可分為四個主要階段：【準備(Preparation)】、【檢測和分析(Detection & Analysis)】、【遏制根除和復原(Containment Eradication & Recovery)】與【事件後活動(Post-Incident Activity)】。



參考來源: NIST SP800-61r2 p.21

(1) 準備階段：所謂事件【準備】之目的，一方面為了在事件發生時建立聯繫、確定程序與收集資安事件資料,以利在事件發生時節省處理時間之外;另一方面也是為了日後相同事件發生前，能夠提前收到告警資訊，以預做防範。

(2) 檢測和分析階段:【檢測】之目的在於協助應變小組判斷事件類別及其影響範圍，以採取有效的緊急應變措施。【分析】之目的，在判斷資安事件等級，並指派合適的人員進行處理與溝通協調。

(3) 遏制根除和復原階段:【遏制】之目的是限制資安事件的影響範圍，某些事件會造成大規模破壞及快速擴散，例如零時差漏洞網路蠕蟲攻擊，在造成更嚴重破壞前,應設法限制其影響程度。【根除】是指清除事件根因，例如修補作業系統安全性漏洞。【復原】目的在於恢復系統的正常操作，須進行系統復原前安全評估，以確保受駭系統及其相關元件已能夠安全正常使用。

(4) 事件後活動階段:【事件後活動】之目的在於瞭解為何事件會發生？如何防止事件重複發生？應執行的改善措施？以及後續的監控與告警措施是否須調整精進？讓惡意行為在活動初期就能夠被發現。

(5) 分析追蹤過程中，發現需提升風險等級時，應依事件(故)升級處理之機制，迅速回應處理。

5、情資分享機制及鑑識資料保存

(1) 資安事件(故)確立後 TCN CERT 將立即進行蒐證,

蒐證內容與報告內容將能透過資安事件(故)資料交換協定與二線 SOC、區域 ISAC 達到資訊交流並透過 Structured Threat Information eXpression(STIX)與 Trusted Automated eXchange of Indicator Information(TAXII)，進行資安事件傳輸格式與傳輸架構，以完備 CERT、SOC 及 ISAC 間的協同合作。

(2) 資安事件(故)各項資訊蒐集與鑑識之電子記錄、書面資料等各種形式的資訊，均應保留 3 年以供後續備查分析使用，並製成案例宣導(去識別化)以利後續強化區域資安人員資安管理作為。

(五) 產官學合作資安培力

1、基層人員資安職能提升

基層機關幾乎完全沒有資訊(安)人力，多數是研考人員兼辦，他們沒有資訊領域的教育背景，行政院及各級機關一直以來都持續辦理相關訓練，問題包括人員流動及如何累進學習階段等，造成課程重複開辦，人員重複上課，結果卻是成效有限，因此，本案將與中部地區大學合作，規劃課程提升基層人員資安職能，目標是能夠傳達類似資安責任等級應辦事項內容，協助說明這些事項的內容以及如何執行的方案。

2、基層維護廠商資安職能提升

基層維護廠商是指基層機關常合作的當地資訊業者，這些人是第一線的維護人員，當機關通報需要協助處理電腦問題時，能多一層認知，辨識是否涉及資安問題，又

或者能配合資安政策，重新安裝電腦時，會依據政策將防毒、軟體派送等代理程式確實安裝設定，這樣就能確保規劃的資安防線不至於產生漏洞，因此，如果可以提升資安職能，將有助於後續的情資蒐集及防禦機制的確保，本案將與中部地區大學合作，規劃課程提升基層維護廠商的資安職能，目標是能夠傳達類似資安責任等級應辦事項內容，協助說明這些事項的內容以及如何執行的方案。

3、資安人才庫建立

因應我國資安威脅日趨嚴峻，資通訊安全已成為我國優先施政的政策項目之一，雖然教育部以結合學術界及產業界能量，與相關部會(經濟部、科技部)協力合作，並結合產官學研資源共同深耕，強化我國資安人才培育量能，但是短期而言，中部地區的資安人才何處尋覓？必須規劃廣泛收集相關資安人才資訊，含括產官學各界，並委託學術單位辦理交流會議，廣納建言，完備資安戰略。

4、合格維護廠商庫

根據第 2 項基層維護廠商資安職能作業，由學術單位建立中彰投直轄縣市內通過課程認證的廠商業者名冊，並予以建立資料庫，以提供中彰投之基層機關洽詢。

5、應變協防

由學術機構參與 TCN-CERT 小組，並廣納產官學專業資安人員為顧問，以協助在中、彰、投發生重大資安事件

時，可以應變協防。

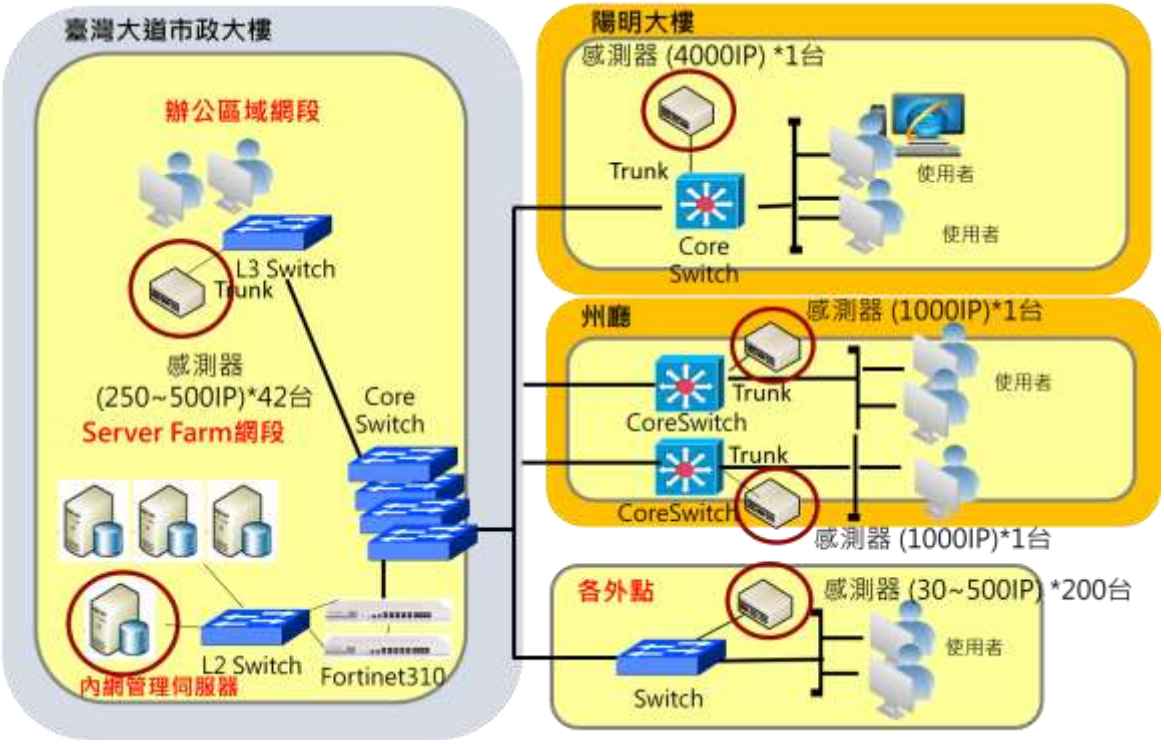
基於上述理念，臺中、彰化、南投縣市政府將聯合產業及學術界舉辦區域性資訊安全訓練，並輔導廠商/人員通過訓練，目標到 109 年至少有 20 家廠商(人員)取得相關證照，取得證照之廠商(人員)資料將納入資安人才資料庫中，並公告於網站上，以利中彰投地區基層機關了解並評估廠商能力之用，另外，自 107 年起每年將舉辦 3 場資訊安全訓練，2 場資安事件處理技術交流會議，並結合大專院校辦理 1 場資安鑑識營隊。

(六) IP 資源管理暨使用行為分析

傳統資安防護多是針對外對內的入侵攻擊，隨著社交工程的盛行、行動裝置的普及，藉由使用者的點擊而觸發或下載惡意程式感染內網電腦，使受害內網電腦成為內部攻擊與擴散的幫兇，使用者私接行動上網裝置，更使內網電腦可不經控管就能連網。一般的資安與網管設備對於外對內的層層把關，也無形提高清楚掌握內網連線設備的難度，近來 IoT 設備的佈署，對於傳統資安威脅的防護與偵測能力更顯捉襟見肘，這些連網行為成為資訊部門管控內網安全的最大挑戰。

臺中市政府自 103 年起啟動 APT 資安專案以來，協助阻擋本府共構網路內對內、內對外異常事件，發現件數所占比例逐年攀升，面對近 2 萬台內網連線設備與 200 餘點的外點 VPN 連線，對於威脅來源的查找受限傳統網管設備的功能常無法即時並精準地排除。本次方案則以導入 IP 資源管理暨使用行為分析系統，提供自動化盤點內部連網設備、填補原有資安、網管設備對於端末設備控管力所不及之處，期能節省

大量人力、時間等在內部網路設備管理、資安處理的成本，以提昇內部連網設備使用的安全性。



圖：IP 資源管理暨使用行為分析系統規劃架構圖

(七) 中彰投機關基於機關差異性聯防需求提報

由臺中市政府提報區域資安聯防共同方案以外，臺中市、彰化縣及南投縣考量政府組織架構及現況需求等條件不同，亟須補強以虛擬系統汰換老舊伺服器、重要雲端系統軟硬體老舊汰換、基層公所防火牆紀錄雲端蒐集、基層公所防火牆紀錄雲端蒐集、基層公所防毒軟體基礎防護、所屬機關 VPN 架構導入預先規劃等，基於機關差異性聯防需求提報部分將以附件方式呈現。

四、 實施範圍

本案之實施範圍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。惟彰化及南投兩縣之鄉鎮市公所補助部分，需待公所同意編列配合款後，該縣政府始同意予以轉補助。

五、 計畫期程

自 108 年 1 月至 109 年 12 月。

六、 關鍵績效指標及年度目標值

(一)臺中市政府

項次	主要績效指標	年度目標
1	汰換老舊資訊軟硬體設備	依補助經費優先從老舊 XP 電腦開始汰換，預計 109 年底前完成，汰換基層公所、衛生、社福等機關老舊已無原廠維護或無法更新之個人電腦或主機等設備，以提升最後一哩的資安防護。 藉由本計畫盤點及汰換老舊軟硬體設備，可以有效提高資安防禦縱深，降低被攻擊成功之風險，提升資安治理成熟度等級，符合中央資安政策及規範。
2	內部風險及威脅管控	於 108 年完成防毒報表系統建置，建構分散式軟體更新派送系統，在同一辦公區同一機關內 10MB 檔案於 2 小時內派送完成，縣市政府共構機房內主機系統每年進行 4 次弱點檢測。 透過風險及威脅管控，可有效降低資安死角及盲點所帶來的危害性。
3	建構自動化區域聯防架構	於 107 年建置完成中彰投縣市政府自動化區域聯防架構，自發現疑似惡意程式，到沙箱檢測確定後，在網路無阻礙情形下，於 30 分鐘內啟動派送到端點作業。 導入自動化區域聯防機制，運用國內業者研發之專家型整合式資安防護產品，不但可以快速防禦，也可以減省基層資安人力之需求，解決部分機關資安人力不足問題。 108 年區域聯防市府所屬機關協防範圍涵蓋率 80%。 109 年區域聯防市府所屬機關協防範圍涵蓋率 90%。
4	情資分享，快速應變及回應	台中市 107 年起每年可以分享 100 條資安情資，彰化縣完成資安事故鑑識調查後，5 工作天內去識別化分享到 NISAC，南投縣 107 年起每年可以分享 20 條資安情資。
5	產官學合作資安培力	中、彰、投縣市政府及聯合產業界、學術界辦理，統計至 109 年輔導 20 家廠商人員通過資安訓練，取得相關資安證照，107 年起每年辦理 3 場區域性資訊安全訓練，2 場資安事件處理技術交流會議，結合大專院校辦理 1 場資安鑑識營隊。
6	國內資安產品或服務採購比率	累計到 109 年至少達 50%(含)以上。

(二)彰化縣政府

項次	主要績效指標	年度目標
1	汰換老舊資訊軟硬	依補助經費優先從老舊 XP 電腦開始汰換，預計 109 年底

	體設備	前完成，汰換基層公所、衛生等機關老舊電腦
2	建構自動化區域聯防架構	於 107 年建置完成中彰投縣市政府自動化區域聯防架構。109 年計畫經費內完成區域內 B 級機關（縣府、警察局、地方稅務局及各地政事務所）資安監控納入區域聯防
3	情資分享，快速應變及回應	完成資安事故鑑識調查後，5 工作天內去識別化分享到 NISAC。
4	產官學合作資安培力	產官學合作資安培力，107 年起每年辦理 3 場區域性資訊安全訓練。
5	國內資安產品或服務採購比率	個人電腦汰換、GCB 管理平台及威脅情資分享共用平台，以國產資安產品為優先採購標的，累計到 109 年至少達 50%(含)以上。

(三)南投縣政府

項次	主要績效指標	年度目標
1	汰換老舊資訊軟硬體設備	依補助經費優先從老舊 XP 電腦開始汰換，預計 109 年底前完成，汰換基層公所、衛生、社福等機關老舊已無原廠維護或無法更新之個人電腦或主機等設備。
2	內部風險及威脅管控	於 108 年完成防毒報表系統建置，建構分散式軟體更新派送系統，在同一辦公區同一機關內 10MB 檔案於 2 小時內派送完成。
3	建構自動化區域聯防架構	於 107 年建置完成中彰投縣市政府自動化區域聯防架構，自發現疑似惡意程式，到沙箱檢測確定後，在網路無阻礙情形下，於 30 分鐘內啟動派送到端點作業。 108-109 年計畫經費內完成縣府、南投戶政及各地政事務所等資安責任等級 B 級機關之資安監控納入區域聯防
4	情資分享，快速應變及回應	南投縣 107 年起每年可以分享 20 條資安情資。
5	產官學合作資安培力	產官學合作資安培力，108 年起，協同台中市、彰化縣，每年辦理 3 場區域性資訊安全訓練。
6	國內資安產品或服務採購比率	累計到 109 年至少達 50%(含)以上。

七、 持續營運評估

本案對於後續維運及運用地方產、學能量的具體作為評估如下：

(一) 情資供給面：

目前台灣資安威脅情資分析研究，行政院國家資通安全會報技術服務中心扮演關鍵角色。在資安即國安的政策下，技服中心的威脅情資應該會持續給區域資安聯防中心使用，並間接提供給本土資安解決方案供應商納入相關產品。

針對臺中市政府資訊中心除會繼續提供給府內機關相關資源外，並擬持續規劃相對應的維運預算，也將與其他地方政府單位合作分享專案情資，以達到持續經營的效用。

(二) 機關資安能量面：

為了強化基層人員的資安意識，亦將要求提供資安服務與解決方案的本土廠商，不定期在地方提供資安講座、教育訓練課程、或資安演習，亦將規劃與在地的學研單位合作推動資安認知。

(三) 廠商資安能量面：

臺中市政府於評估選用資安服務或解決方案時，優先採用本土優良廠商，著重在地服務與過去實績。

資安解決方案提供商需能做為第二線技術支援角色，提供資安服務廠商相應的威脅偵測或事件處理工具，並持續透過教育訓練方式將最新的威脅資訊與技術，傳遞給資安服務廠商與區域聯防中心資安小組。

資安服務提供商需具備第一線技術服務與事件處理的能力，並持續與區域聯防中心配合，提供基層人員或各縣市防禦中心的資安團隊相關教育訓練課程。

依據前述規劃之實施範圍及工作項務，考量「資安亦國防」的原則，與連結在地能量、扶持本土資安廠商的理念，大部分採用國內的資安廠商產品與服務，建置區域聯防中心，在價格及服務上都比較優惠，因此，只要參與區域資安聯防的機關能夠編列些許預算及有一顆要把資安做好的心，一定能夠達到持續維運的目標。

八、 經費明細概算

(一)臺中市政府：

單位：新臺幣

年度	項次	工作項目	工作內容	所需經費		績效目標	優先次序(必填)
				經常門	資本門		
108	1	GCB 導入服務及管理工具授權	延續 107 年 GCB 導入工作，擴大導入機關，並購置管理工具授權		7,000,000	1.可達成行政院實地稽核技術檢測之組態設定安全防護檢測之目標。及本案之績效指標第 2 項。 2.強化端點設備安全性	1
	2	整合式防護服務 DDA	沙箱分析設備，具備多個動態威脅分析器，驅動可疑程式樣本行為重演，判別惡意的C&C 中繼站位址，自動回	1,800,000		自動研判可疑程式樣本快速產出威脅情資 自動派送威脅情資到本地情資中心	2

		後續維運	饋設備進行本地端防護，提供惡意威脅的執行和評估摘要報告，可匯出樣本檔案提交病毒碼製作			可匯入 STIX 威脅情資 接受手動上傳可疑檔案並進行分析	
	3	分散式軟體派送服務	常用軟體更新、修補程式派送等	1,400,000		1.建置導入後，可以符合應辦事項之安全性檢測—資安健診—使用者端電腦檢視項目，具有經常性查核功能，確保常態符合規定。也可達成行政院實地稽核技術檢測之使用電腦安全防護檢測之應用軟體更新。 2.有效減少漏洞存在時間，防止駭客利用及攻擊。	3
	4	加解密服務平台後續維護	加密訊息解密(SSL/TLS Offloading)，減輕現有網管設備(F/W, IPS)的負擔，並提高資安設備分析的效能	600,000		駭客已進化，設備被遠端控制，在內網活動或加密打包隱藏，現有資安防堵方式無法防禦。 SSL/TLS Offloading 可以減輕現有網管設備的負載，解封後的資料，送給資安設備判讀，有助於蒐集威脅情資，進行防禦。	4
	5	弱點評	主機弱點檢測服務	1,500,000		本府 400 台以上主機弱掃除產出報告	5

		估檢測服務				外，還能建檔追蹤歷史弱點及修補情形。	
	6	中彰投區域聯防中心維運	1.國內外威脅情資蒐集與通報 2.資安緊急事件應變處理 3.區域聯防運作與通報 4.區域聯防中心維運	1,900,000		每月初提供前一個月維運報告。 每一季召開季檢討會議。 年度結束前提出年度成果報告。	6
	7	產官學提升資安培力服務	與中部區域大學合作辦理 1.基層人員資安職能提升訓練服務 2.基層維護廠商資安職能提升訓練服務 3.資安人才庫管理系統與合格維護廠商系統 4.專責資安人員職能提升訓練服務	350,000		中、彰、投縣市政府及聯合產業界、學術界辦理，統計至 109 年輔導 20 家廠商人員通過資安訓練，取得相關資安證照，107 年起每年辦理 3 場區域性資訊安全訓練，2 場資安事件處理技術交流會議，結合大專院校辦理 1 場資安鑑識營隊。	7
	8	日誌分析服務	建置日誌蒐集分析系統，並維運分析內外部資安情資	1,360,000		依據蒐集日誌資料，建置單一入口網，並於該系統直覺化取得相關戰情情資呈現。	8
	9	進階網路安全	能即時偵測、分析及回應今日隱匿的鎖定目標式攻擊。是一種比 SOC 更能	900,000		導入後可以達成應辦事項—防禦縱深之 APT 攻擊防禦項目	9

		監控DDI	即時回應攻擊的服務。				
	10	資安日誌平台	收納與關聯相關原始日誌(syslog)、支援弱點結果關聯功能、資安日誌情資分析、流量分析	600,000		強化區域聯防資安防護，以及蒐集情資。	10
	11	NFV 網路資安功能虛擬化	臺中市政府共構網路		7,480,000	NFV 將既有專用網路設備的功能以軟體的方式虛擬化，並經由雲端運算(Cloud Computing)相關技術實現，藉此可快速、靈活與彈性的部署網路業務，縮短設備配置週期，降低硬體建置與維運的成本，有助於區域聯防動態彈性調配。	11
	12	IP 資源管理暨使用行為分析系統導入	IP 資源管理暨使用行為分析系統導入、整合 AD 管理、網路連線申請流程、系統安裝建置服務、外點安裝建置服務。		11,230,000	1.可達成行政院實地稽核技術檢測之組態設定安全防護檢測之目標。及本案之績效指標第 2 項。 2.強化端點設備安全性	12
	13	汰換老	汰換老舊個人電腦		8,000,000	汰換基層公所、衛生、社福等機關老舊	13

		舊個人電腦				電腦	
	小計			10,410,000	33,710,000		
109	1	GCB 導入服務及管理工具授權	延續 107 年 GCB 導入工作，擴大導入機關，並購置管理工具授權		7,600,000	1.可達成行政院實地稽核技術檢測之組態設定安全防護檢測之目標。及本案之績效指標第 2 項。 2.強化端點設備安全性	1
	2	整合式防護服務 DDA 後續維運	沙箱分析設備，具備多個動態威脅分析器，驅動可疑程式樣本行為重演，判別惡意的C&C 中繼站位址，自動回饋設備進行本地端防護，提供惡意威脅的執行和評估摘要報告，可匯出樣本檔案提交病毒碼製作	1,800,000		自動研判可疑程式樣本快速產出威脅情資 自動派送威脅情資到本地情資中心 可匯入 STIX 威脅情資 接受手動上傳可疑檔案並進行分析	2

	3	分散式軟體派送服務	常用軟體更新、修補程式派送等	1,400,000		1.建置導入後，可以符合應辦事項之安全性檢測—資安健診—使用者端電腦檢視項目，具有經常性查核功能，確保常態符合規定。也可達成行政院實地稽核技術檢測之使用電腦安全防護檢測之應用軟體更新。 2.有效減少漏洞存在時間，防止駭客利用及攻擊。	3
	4	加解密服務平台後續維護	加密訊息解密(SSL/TLS Offloading)，減輕現有網管設備(F/W, IPS)的負擔，並提高資安設備分析的效能	600,000		駭客已進化，設備被遠端控制，在內網活動或加密打包隱藏，現有資安防堵方式無法防禦。 SSL/TLS Offloading 可以減輕現有網管設備的負載，解封後的資料，送給資安設備判讀，有助於蒐集威脅情資，進行防禦。	4
	5	弱點評估檢測服務	主機弱點檢測服務	1,500,000		本府 400 台以上主機弱掃除產出報告外，還能建檔追蹤歷史弱點及修補情形。	5
	6	中彰投	1.國內外威脅情資蒐集與通報	1,900,000		每月初提供前一個月維運報告。	6

		區域聯防中心維運	2.資安緊急事件應變處理 3.區域聯防運作與通報 4.區域聯防中心維運			每一季召開季檢討會議。 年度結束前提出年度成果報告。	
	7	產官學提升資安培力服務	與中部區域大學合作辦理 1.基層人員資安職能提升訓練服務 2.基層維護廠商資安職能提升訓練服務 3.資安人才庫管理系統與合格維護廠商系統 4.專責資安人員職能提升訓練服務	350,000		中、彰、投縣市政府及聯合產業界、學術界辦理，統計至 109 年輔導 20 家廠商人員通過資安訓練，取得相關資安證照，107 年起每年辦理 3 場區域性資訊安全訓練，2 場資安事件處理技術交流會議，結合大專院校辦理 1 場資安鑑識營隊。	7
	8	日誌分析服務	建置日誌蒐集分析系統，並維運分析內外部資安情資	1,360,000		依據蒐集日誌資料，建置單一入口網，並於該系統直覺化取得相關戰情情資呈現。	8
	9	進階網路安全監控 DDI	能即時偵測、分析及回應今日隱匿的鎖定目標式攻擊。是一種比 SOC 更能即時回應攻擊的服務。	900,000		導入後可以達成應辦事項—防禦縱深之 APT 攻擊防禦項目	9
	10	資安日誌平台	收納與關聯相關原始日誌(syslog)、支援弱點結果關聯功能、資安日誌情資分析、流量分析	600,000		強化區域聯防資安防護，以及蒐集情資。	10

	11	汰換老舊個人電腦	汰換老舊個人電腦		5,375,000	汰換基層公所、衛生、社福等機關老舊電腦	11
	12	IP 資源管理暨使用行為分析系統導入	IP 資源管理暨使用行為分析系統導入、整合 AD 管理、網路連線申請流程、系統安裝建置服務、外點安裝建置服務。	1,865,000		1.可達成行政院實地稽核技術檢測之組態設定安全防護檢測之目標。及本案之績效指標第 2 項。 2.強化端點設備安全性	12
	小計			12,275,000	12,975,000		
合　　計				69,370,000 元			

(二) 彰化縣政府：

單位：新臺幣

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		

							（必填）
108	1	進階網路安全監控 DDI	即時偵測、分析及回應今日隱匿的鎖定目標式攻擊。	600,000		建構自動化區域聯防架構	1
	2	威脅情資分享共用平台(含駐點人力)	威脅情資包括：中毒、DDI、SOC 通報、技服通報、預警通報等情資	1,900,000		情資分享，快速應變及回應	2
	3	汰換基層軟硬體設備	汰換基層公所、衛生單位老舊資訊設備（伺服器、個人電腦及防火牆）並導入 GCB 服務	3,000,000	38,925,000	汰換基層老舊硬體設備並導入 GCB	3
	4	郵件過濾裝置	汰換郵件過濾裝置		3,630,000	建構自動化區域聯防架構並完成應辦事項-資通安全防護	4
	5	GCB 服務導入及雲端機房儲存設備	本府 GCB 服務導入及提供基層公所網站共構資料儲存使用	400,000	1,398,000	GCB 服務導入	5
	6	核心系統硬體擴充汰換	汰換核心資訊系統-公文系統老舊硬體設備並提供衛生局、基層公所公文管理及檔案儲存空間		11,447,000	汰換核心資訊系統老舊硬體設備	6

	7	防毒軟體	企業安全套件及端點安全模組		600,000	建構自動化區域聯防架構並完成應辦事項-資通安全防護	7
	8	產官學提升資安培力服務	與中部區域大學合作辦理，提升基層人員資安職能	350,000		產官學合作資安培力	8
	小計			6,250,000	56,000,000		
109	1	進階網路安全監控 DDI	即時偵測、分析及回應今日隱匿的鎖定目標式攻擊。	600,000		建構自動化區域聯防架構	1
	2	威脅情資分享共用平台(含駐點人力)	威脅情資包括：中毒、DDI、SOC 通報、技服通報、預警通報等情資	1,900,000		情資分享，快速應變及回應	2
	3	GCB 服務導入維運	本府 GCB 服務導入維運	500,000		GCB 服務導入	3
	4	安全性檢測	警察局辦理資安健診、滲透測試等應辦事項	500,000		完成應辦事項- 安全性檢測	4
	5	監控管理	本府、警察局、地方稅務局及各地政事務所	2,520,000		完成應辦事項- 監控管理	5
	6	ISMS 推動作業	資安責任等級 B 級機關警察局、地方稅務局及各地政事務所核心系統辦理 ISMS 推動維運作業	2,400,000		完成應辦事項- ISMS 推動作業	6

	7	核心系統改版建置	核心資訊系統-表單系統改版建置並導入資通系統防護基準控制措施		4,000,000	完成應辦事項- 資通系統分級及防護基準	7
	8	產官學提升資安培力服務	與中部區域大學合作辦理，提升基層人員資安職能	75,000		產官學合作資安培力	8
	小計			8,495,000	4,000,000		
合　　計				74,745,000 元			

(三) 南投縣政府:

單位：新臺幣

年度	項次	工作項目	工作內容	所需經費		績效目標	**優先次序(必填)**
				經常門	資本門		
108	1	南投縣政府暨所屬機關 GCB	GCB 公告 400 條導入，內容涵蓋－ 1.人力導入 2.輔助工具	500,000		1.可達成行政院實地稽核技術檢測之組態設定安全	2

		導入	3.教育訓練 4.排除條目說明			防護檢測之目標。及本案之績效指標第 2 項。 2.強化端點設備安全性。	
	2	網頁應用程式防火牆(WAF)導入	導入 100M 之網頁應用程式防火牆	230,000		1.可以符合 A.B 資安等級應辦事項。 2.強化資安防護縱深，提高駭客攻擊難度。	19
	3	分散式軟體派送服務	常用軟體更新、修補程式派送等	520,000		1.建置導入後，可以符合應辦事項之安全性檢測—資安健診—使用者端電腦檢視項目，具有經常性查核功能，確保常態符合規定。也可達成行政院實地稽核技術檢測之使用電腦安全防護檢測之應用軟體更新。 2.有效減少漏洞存在時間，防止駭客利用及攻擊。	37
	4	進階網路安全防護 DDI	能即時偵測、分析及回應今日隱匿的鎖定目標式攻擊。是一種比 SOC 更能即時回應攻擊的裝置。 *高偵測率 — 獨特的偵測引擎和客製	600,000		建構自動化區域聯防架構	9

			化沙盒模擬分析(Sandboxing)。 *深入的分析 — 結合本地端及全球的威脅關聯情報。 *快速的回應 — 利用進階端點鑑識分析技術與共享的入侵指標（IOC）情報。				
	5	中彰投區域聯防中心維運	1.國內外威脅情資蒐集與通報 2.資安緊急事件應變處理 3.區域聯防運作與通報 4.區域聯防中心維運	1,900,000		建構自動化區域聯防架構	12
	6	汰換老舊主機	本案工作項目		2,400,000	基層公所、衛生、社福單位-Windows 2003 Server	25
	7	汰換老舊個人電腦	本案工作項目		11,925,000	基層公所、衛生、社福單位-Windows XP 電腦	28
	8	衛生局虛擬系統(汰換老舊實體主機)	VMware vSphere Essentials Plus *1 + Server *3 + SAN *1+ Storage *1		1,324,000	以建置虛擬系統方式汰換老舊主機，連帶簡化資訊系統備份問題，以強化資訊安全。	15

	9	汰換本府對 VPN 二級機關建立 IPsec 加密通道設備	汰換本府對 VPN 二級機關建立 IPsec 加密通道設備	510,000		1.落實系統管理向上集中化之精神。 2.本府對 VPN 二級機關建立 IPsec 加密通道設備，使用期間長達 14 年，早已逾法定使用年限，可靠性堪憂，爰藉由本案提昇機關連線之可靠性。	49
	小計			4,260,000	15,649,000		
109	1	南投縣政府暨所屬一、二級機關 GCB 導入	GCB 公告 400 條導入，內容涵蓋－ 1.人力導入 2.輔助工具 3.教育訓練 4.排除條目說明	500,000		1.可達成行政院實地稽核技術檢測之組態設定安全防護檢測之目標。及本案之績效指標第 2 項。 2.強化端點設備安全性。	3
	2	鄉鎮市公所 GCB 導入	GCB 公告 400 條導入，內容涵蓋－ 1.人力導入 2.輔助工具 3.教育訓練 4.排除條目說明	1,300,000		1.可達成行政院實地稽核技術檢測之組態設定安全防護檢測之目標。及本案之績效指標第 2 項。	4

						2.強化端點設備安全性。	
	3	網頁應用程式防火牆(WAF)導入	導入100M之網頁應用程式防火牆	230,000		1.可以符合A.B資安等級應辦事項。 2.強化資安防護縱深，提高駭客攻擊難度。	20
	4	分散式軟體派送服務	常用軟體更新、修補程式派送等	600,000		1.建置導入後，可以符合應辦事項之安全性檢測—資安健診—使用者端電腦檢視項目，具有經常性查核功能，確保常態符合規定。也可達成行政院實地稽核技術檢測之使用電腦安全防護檢測之應用軟體更新。 2.有效減少漏洞存在時間，防止駭客利用及攻擊。	38
	5	鄉鎮市公所分散式軟體派送服務	常用軟體更新、修補程式派送等	1,040,000		1.建置導入後，可以符合應辦事項之安全性檢測—資安健診—使用者端電腦檢視項目，具有經常性查核功能，確保常態符合規定。也可達成行政院實地稽核技術檢測之使用電腦安全防護檢測之應用軟體更新。	40

						2.有效減少漏洞存在時間，防止駭客利用及攻擊。	
	6	進階網路安全防護 DDI	能即時偵測、分析及回應今日隱匿的鎖定目標式攻擊。是一種比 SOC 更能即時回應攻擊的裝置。 *高偵測率 — 獨特的偵測引擎和客製化沙盒模擬分析(Sandboxing)。 *深入的分析 — 結合本地端及全球的威脅關聯情報。 *快速的回應 — 利用進階端點鑑識分析技術與共享的入侵指標（IOC）情報。	600,000		建構自動化區域聯防架構	10
	7	中彰投區域聯防中心維運	1.國內外威脅情資蒐集與通報 2.資安緊急事件應變處理 3.區域聯防運作與通報 4.區域聯防中心維運	1,900,000		建構自動化區域聯防架構	13
	8	加解密服務平台	加密訊息解密(SSL/TLS Offloading)，減輕現有網管設備(F/W, IPS)的負擔，並提高資安設備分析的效能 (SSL 是造成近年來大量惡意軟體，特別	4,000,000		內部風險及威脅管控	14

			是綁架勒索攻擊，如 CryptoLocker 、TeslaCrypt 等發生的主要元兇,藉由該設備可將 SSL/TLS 解密/加密提供更具擴充的可視性功能,並可管理加密流量，協助檢測出潛伏惡意程式、資料竊取攻擊、指令與控制等威脅）				
	9	雲端型整合式威脅防護閘道 CloudEdge 服務	導入雲端監控服務	1,040,000		導入後可以達成應辦事項—防禦縱深之 APT 攻擊防禦項目 本項雲端型資安服務，功能廣泛，價格親民，有利於基層機關有限預算下執行，符合本案永續營運規劃之評估原則。	42
	10	汰換老舊主機	本案工作項目		2,600,000	基層公所、衛生、社福單位- Windows 2003 Server	26
	11	汰換老舊個人電腦	本案工作項目		13,675,000	基層公所、衛生、社福單位-Windows XP 電腦	29
	12	汰換老舊防火	本案工作項目		716,000	基層公所、衛生、社福單	17

		牆 <2.5G Gbps				位。	
	13	汰換老舊防火牆 <8GGbps	本案工作項目		600,000	基層公所、衛生、社福單位。	18
	14	基層公所防火牆 LOG 集中管理分析系統維運	N-Reporter 維運	40,000		基層公所防火牆紀錄集中蒐集管理，提升資安。	23
	小計			11,250,000	17,591,000		
合　　計				48,750,000 元			

註：

1. 本表可依需求增列。
2. 請詳列各工作內容、經費編列及對應績效目標，多項工作對應單一績效目標時，請於備註欄說明。

九、 經費補助表

(一)臺中市政府

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	行政院資通安全處補助款
108	44,120,000	_	17,648,000	26,472,000
109	25,250,000	_	10,100,000	15,150,000

(二)彰化縣政府

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	行政院資通安全處補助款
108	62,250,000		12,450,000	49,800,000
109	12,495,000		2,499,000	9,996,000

(三)南投縣政府

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	行政院資通安全處補助款
108	19,909,000	-	3,982,000	15,927,000
109	28,841,000	-	5,768,000	23,073,000

(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
108	44,120,000	62,250,000	19,909,000
109	25,250,000	12,495,000	28,841,000
小計	69,370,000	74,745,000	48,750,000
合計			192,865,000

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)	
108	63.6%	44,120,000	108 年 11 月期末成果報告
109	100%	69,370,000	109 年 11 月期末成果報告

(二)彰化縣政府

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
108	83.28	62,250,000	完成資安事故鑑識調查後，5 工作天內去識別化分享到 NISAC。
109	100	74,745,000	個人電腦汰換、GCB 管理平台及威脅情資分享共用平台，以國產資安產品為優先採購標的，累計到 109 年至少達 50%(含)以上

(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
108	40.84%	19,909,000	108.12 導入本府及所屬一級機關 GCB，搭配汰換老舊主機、PC，完成目標值
109	100%	48,750,000	109.12 導入公所 GCB、搭配汰換老舊主機、PC，完成目標值

十一、預期效益

資安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。臺中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，並切合本土資安產業發展需求。

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) 強化基層機關個人電腦作業系統安全，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。

(二) 聯結外部雲端威脅情資，建立區域式的在地聯防能量，納入關聯的情資包括國家的資安研發能量，如行政院國家資通安全會報技術服務中心，與本土資安廠商匯整的全球威脅情蒐資訊等。充分的利用全球與全國的威脅資訊，與區域式的視野與資源共享，達到快速應變及即時處理目標，大幅提升各縣市的數位防禦能力。

(三) 強化網路端資安設備防禦能量，防堵或封鎖駭客入侵管道，避免公務重要資料被駭客入侵，甚至影響民眾權益，進一步提高政府服務的民眾信賴度。

(四) 參與本計畫之專案駐點人員將取得寶貴的區域聯防經驗，並且更熟悉縣市政府內部實際的資安維運作業，目前，中部地區非常欠缺資安人才，未來不論是機關有約聘雇或是產業界有相關職缺，都會優先進用。

(五) 資安與數位產業並重，皆是重點扶植的臺灣產業，本計畫加強使用國內資安產品，從需求應用端來帶動市場，並以台灣研發為優先，有效扶植國內資安產業的發展，間接促進民間資安自主研發的能量。

十二、 相關聯絡資料

縣市政府	機關	聯絡人姓名	電話	E-mail
臺中市政府	資訊中心	張碧顯	04-22289111 #22301	ps491@taichung.gov.tw
彰化縣政府	計畫處	許宏基	04-7531351	a230400@email.chcg.gov.tw
南投縣政府	計畫處 資訊管理科	周湧裕	049-2245361	ian@nantou.gov.tw

附件 7

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之分項計畫

臺南市

108年3月

臺南市政府

前瞻基礎建設計畫-數位建設-強化政府基層機關資安防護及區域聯防計畫

一、計畫緣起

因應行政院 106 年 4 月 5 日核定通過之「前瞻基礎建設計畫」，其中「數位建設」子項目-「強化政府基層機關資安防護及區域聯防」須提出競爭型計畫以爭取中央補助，並考量地方政府資安事件頻傳，確有加強資安區域聯防之必要，而國際情勢相關資安事件亦層出不窮（如一銀提款機遭駭事件，WannaCry 勒索病毒肆虐全球事件），本府爰結合雲林縣及嘉義縣市等鄰近區域縣市政府及產學界共同提案以強化基層機關之資安防護，提升基層機關之資訊服務能量、建置區域資安聯防、加強資安防禦縱深及創新服務整合並研提持續營運規劃，亦期能有助於帶動資安產業發展，特擬訂本計畫。

二、計畫目標

(一) 與行政院資通安全處合作研擬強化基層機關之資安防護之方案，建構符合政府組態基準(GCB)之要求。

(二) 提升基層公所之資訊服務能量，俾利智慧城市之數位內涵建設。

(三) 研提自籌維運規劃，以因應資安防護之持續營運。

(四) 強化寬頻網路之資安防護建設。

(五) 建置區域資安聯防及服務整合，落實區域治理成效。

(六) 優先使用國內自主研發之資安產品，以帶動資安產業發展。

三、實施範圍

有關各計畫之實施對象及實施區域，說明如下：

(一) 汰換基層機關(公所社政及衛政)7 年以上電腦設備，以各縣市基層機關(公所、社政及衛政單位)為實施範圍。

(二) 建置區域聯防情資分享機制，以區域內縣市(雲林縣、嘉義縣、嘉義市及台南市政府)共同建立情資分享團隊共享相關資安情資。

(三) 加強資安防禦縱深，購置資安設備，分別由各縣市調查所屬機關需求，故以縣市政府所屬機關為實施範圍。

(四) 研提創新應用，分別由各縣市調查所屬機關需求，故以縣市政府所屬機關為實施範圍。

四、關鍵績效指標及年度目標值

雲林縣:

項次	主要績效指標	年度目標	權重	如何完成預期目標
1	汰換基層機關(公所社政及衛政)7年以上電腦設備	107 年底完成4計80台個人電腦,108年底完成 30% 計396 台個人電腦,109年底完成100%計935台個人電腦及42 台伺服器,合計 1411 台個人電腦及42台伺服器	63%	請相關單位依經費執行年度完成採購、安裝及原設備汰換事宜。
2	建置區域聯防情資分享機制	107~109 逐年完成40%、59%、100%	22%	請相關單位依經費執行年度完成採購及建置事宜。
3	加強資安防禦縱深，購置資安設備	109 年底完成100%	3%	請相關單位依經費執行年度完成採購、安裝及原設備汰換事宜。
4	研提創新應用，強化資安機制	創新服務-GCB 管理系統建置,107年底完成B級機關100%,108年完成 C 級機關50%，109年完成 C 級機關100%	12%	請相關單位依經費執行年度完成採購、安裝及原設備汰換事宜。

嘉義縣:

項次	主要績效指標	年度目標	權重	如何完成預期目標
1	汰換基層機關(公所社政及衛政)7 年	1.107年底完成汰換衛政、社政PC 100%。 2.108年底完成汰換公所PC 30%,	30%	請相關單位依經費執行年度完成採購、安裝及原設備汰換事宜。

	以上電腦設備	3.109 年底完成汰換公所 pc 及衛、社、公所主機伺服器設備 100%。		
2	建置區域聯防情資分享機制	107~109 逐年完成 30、30、40%	20%	請相關單位依經費執行年度完成採購及建置事宜。
3	加強資安防禦縱深，購置資安設備	107-109 逐年完成 15%、20%、65%	30%	請相關單位依經費執行年度完成採購、安裝及原設備汰換事宜。
4	研提創新應用，強化資安機制	創新服務- 1.107 年底完成 GCB 管理系統建置及 B 級機關 GCB 政策導入。	20%	請相關單位依經費執行年度完成採購、安裝及原設備汰換事宜。

嘉義市:

項次	主要績效指標	目標	權重	如何完成預期目標
1	汰換資訊軟硬體設備(7年以上)	完成伺服器主機汰換	5%	汰換伺服器主機 8 台
2		完成個人電腦汰換	10%	汰換個人電腦 141 台
3	建置區域聯防 ISAC 機制	建立 ISAC 區域聯防情資與防護規則派送系統	15%	建構本府轄下機關與鄰近縣市成立資安互聯網，分享情資資訊及防護規則。
4		建立資安事件快速應變小組及處理流程	10%	結合本府與所屬機關共 9 個單位成立資安事件快速應變小組，與區域聯防中心整合
5		教育訓練與產學合作	5%	每年舉辦資安教育訓練以熟悉監控管理，產學合作分長短期每年舉辦資安實習交流。
6	強化資安防護縱深設備，健全機關資安環境防護	完成資安設備汰換與建置資安防護	10%	建置情資分享系統、端點 APT 防護，及強化資通網路資安設備防護能量。
7		主機系統與網站弱點掃描服務、滲透測試、資安健診	10%	提升基層公所及社政、衛政機關資安防護水準，針對核心系統主機、網站弱點掃描及對外核心資訊網站滲透測試、資安健診服務，強化資安體質。
8		防毒軟體及閘道	5%	完成機關用戶端防毒軟體安裝及佈署監控機制。
9		建立 SOC 區域聯防監控系統	10%	完成本府資安等級 B 級 3 個機關建置 SOC 區域聯防監控系統，涵蓋基層公所及社政單位。
10		區域聯防情資派送建置	5%	完成 8 個外點機關跨區域整合彙整資訊與威脅分析。

11	研提創新應用，強化資安機制	網路流量監控與負載平衡系統	5%	本府與所屬機關(VPN)內部網路的對外網路流量管理監控。
12		開放式軟體管理平台	5%	完成建置本府暨所屬機關 4 個單位軟體雲端平台，以有效管理軟體授權與資安管控。
13		機房雲端資源服務	5%	完成內網與 DMZ 各建置超融合基礎架構平台

台南市:

項次	主要績效指標	年度目標	權重	如何完成預期目標
1	汰換基層機關(公所社政及衛政)7 年以上電腦設備	108 年底完成 Windows 2003 Server 汰換 33 台	30%	請相關單位依經費執行年度完成採購、安裝及原設備汰換事宜。
2	建置區域聯防情資分享機制	109 年底完成 100%	20%	請相關單位依經費執行年度完成採購及建置事宜。
3	加強資安防禦縱深，購置資安設備	109 年底完成 100%	30%	請相關單位依經費執行年度完成採購、安裝及原設備汰換事宜。
4	研提創新應用，強化資安機制	AD 及 GCB 創新應用服務 108 年底完成 100%	20%	請相關單位依經費執行年度完成採購、安裝及原設備汰換事宜。

本區區域聯防工作內容包含：

- 雲嘉嘉南區域各機關一線 SOC 資安監控通報
- 雲嘉嘉南區域 ISAC 情資分享機制
- 雲嘉嘉南區資安緊急應變機制
- 雲嘉嘉南區域二線 SOC 分析關聯通報

區域聯防 KPI 總表：

	108 年	109 年
臺南市政府	80%	90%
嘉義市政府	80%	90%
嘉義縣政府	80%	90%
雲林縣政府	80%	90%
範圍及說明	涵蓋範圍：縣市政府、衛政、社政、各鄉鎮區公所等。 說明：依達成區域聯防工作內容機關數比例換算，估略完成進度至少為 80%。	涵蓋範圍：縣市政府、衛政、社政、各鄉鎮區公所等 說明:依達成區域聯防工作內容機關數比例換算,估略完成進度至少為 90%。

五、持續營運評估

本計畫期程結束後，後續維運方式依各縣市政府經費狀況，說明如下：

(一) 汰換基層機關(公所社政及衛政)7 年以上電腦設備

1. 雲林縣：由各使用機關每年編列預算維護，維護費約原購置經費 10%，約 3,948 千元。
2. 嘉義縣：由各使用機關每年編列預算維護，維護費約原購置經費 10%，約 2,500 千元。
3. 嘉義市：由各使用機關每年編列預算維護，維護費約原購置經費 10%，約 300 千元。
4. 台南市：由各使用機關每年編列預算維護，維護費約原購置經費 10%，約 780 千元。

(二) 建置區域聯防情資分享機制

1. 雲林縣：由各使用機關每年編列預算維護，約 550 千元。
2. 嘉義縣：由各使用機關每年編列預算維護，約 2,968 千元。
3. 嘉義市：由各使用機關每年編列預算維護，約 1,150 千元。
4. 台南市：由各使用機關每年編列預算維護，約 3,286 千元。

(三) 加強資安防禦縱深，購置資安設備

1. 雲林縣：由各使用機關每年編列預算維護，約 187 千元。
2. 嘉義縣：由各使用機關每年編列預算維護，約 2,200 千元。
3. 嘉義市：由各使用機關每年編列預算維護，約 3,500 千元。
4. 台南市：由各使用機關每年編列預算維護，約 1,308 千元。

(四) 研提創新應用，強化資安機制

1. 雲林縣：共構建置部分由縣府編列預算維護，各機關部分，由各機關每年編列預算維護，約 530 千元。
2. 嘉義縣：共構建置部分由縣府編列預算維護，各機關部分，由各機關每年編列預算維護，約 1,800 千元。
3. 嘉義市：共構建置部分由市府編列預算維護，各機關部分，由各機關每年編列預算維護，約 1,350 千元。
4. 台南市：共構建置部分由市府編列預算維護，各機關部分，由各使用機關每年編列預算維護，約 1,198 千元。

六、經費明細概算

（一）、雲林縣：

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		
108	1	汰換基層機關(公所、社政、衛政)7年以上電腦設備	汰換個人電腦(396台)		9,900,000	降低資安風險	1
	2	前瞻計畫資安防護區域聯防服務(ISAC)暨資訊安全監控中心(SOC)	建置區域聯防情資分享機制以及24小時即時資安監控服務與事件處理(實施範圍公所、衛政、社政)	2,475,000		區域聯防監控	2
	3	創新服務-所屬及公所GCB導入	跨site GCB管理系統建置	500,000		創新服務	3
109	1	汰換基層機關(公所、社政、衛政)7年以上電腦設備	汰換個人電腦(935 台)及伺服器(42台)		27,575,000	降低資安風險	1
	2	前瞻計畫資安防護區域聯防服務(ISAC)暨資訊安全監控中心(SOC)	建置區域聯防情資分享機制以及24小時即時資安監控服務與事件處理(實施範圍公所、衛政、社政)	5,630,000		區域聯防監控	2
	3	創新服務-所屬及公所GCB導入	跨site GCB管理系統建置	1,870,000		創新服務	3
	4	汰換基層機關(公所、衛政)防火牆	汰換無法支援防護規則自動派送防火牆(13台)		1,975,000	強化資安防護縱深設備	4
合　　計				49,925,000元			

嘉義縣：

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		
108年度	1	汰換基層機關(公所社政及衛政)7年以上電腦設備	更換基層機關(公所社政及衛政)7年以上電腦設備	0	4,562,000	108年底前完成汰換基層pc電腦100%以上	1
	2	建置區域聯防情資分享機制	建置區域聯防情資分享機制	500,000	0	配合行政院政策	4
	3	加強資安防禦縱深，購置資安設備	建置智慧共構機房收納公所系統、網路安全設備	0		配合區域聯防、收納公所資訊系統等設備建置	2
			落實各項資安責任等級應辦事項(含SOC資安監控、資安健診、主機網站弱掃、防毒、郵件過濾、資安人力服務)		0	資安責任等級要求	3
			更換衛、社政防火牆設備				7
	4	研提創新應用，強化資安機制	(1) 建置全縣電子郵件系統，提供APT防護			資安責任等級要求	6

			(2) 建置網頁資料流加解密		7,000,000		
			(3) GCB 軟體維護	1,722,000	0		5
109 年度	1	汰換基層機關(公所社政及衛政)7 年以上電腦設備	更換基層機關(公所社政及衛政)7 年以上主機伺服器設備	0	15,438,000	109 年底前完成汰換基層主機設備 100%	1
	2	建置區域聯防情資分享機制	建置區域聯防情資分享機制	2,055,500	0	配合行政院政策	4
	3	加強資安防禦縱深，購置資安設備	建置智慧共構機房(收納公所系統、網路安全設備、頻寬升級納管)	0		配合區域聯防、收納公所資訊系統等設備建置	2
			落實各項資安責任等級應辦事項(含 SOC 資安監控、資安健診、主機網站弱掃、防毒、郵件過濾、防火牆阻擋、資安人力服務)	2,055,500	0	資安責任等級要求	3
	4	研提創新	(1) 建置弱點			資安責任等級要	6

		應用，強化資安機制	管理中心			求	
			(2) GCB 軟體維護	2,000,000	0		5
合　　計				$28,333,000 元			

嘉義市：

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	優先順序
				經常門	資本門		
108	1	個人電腦	57 台	0	1,425,000	汰換資訊軟硬體設備(7 年以上)	1
	2	汰換伺服器	8 台	0	1,600,000		2
	3	ISAC 區域聯防機制服務系統	1. 區域聯防情資與防護規則派送系統 2. 建立資安事件快速應變小組及處理流程 3. 結合地區大學能量合作	2,857,000	0	建置區域聯防 ISAC 機制	3
	4	SOC 監控系統	24 小時即時資安監控服務與事件處理	2,000,000	0	強化資安防護縱深設備	4
	5	IP 資安情資分析設備	1 台(資安事件回報系統)	0	2,400,000		5
	6	整體及端點 APT 防護服務	內部設備端點資安防護	0	2,500,000		6
	7	網路流量監控與負載平衡系統	網路流量負載平衡	0	1,600,000	研提創新應用	7
	8	開放式	1200 台導入軟體	0	2,618,000		8

		軟體管理平台	雲端平台				
109	1	ISAC 區域聯防機制服務系統	1. 區域聯防情資與防護規則派送系統 2. 建立資安事件快速應變小組及處理流程 3. 結合地區大學能量合作	2,850,000	0	建置區域聯防 ISAC 機制	1
	2	SOC 監控系統	24 小時即時資安監控服務與事件處理	2,000,000	0	強化資安防護縱深設備	2
	3	主機系統與網站弱點掃描服務、滲透測試、資安健診	伺服主機及網站弱點掃描、電腦設備資安健診	2,620,000	0		3
	4	防毒軟體	防毒閘道及用戶端防毒軟體	530,000	0		4
	5	機房雲端資源服務	本府暨所屬機關內網及 DMZ 虛擬化平台實體主機簡化作業	0	10,714,000	研提創新應用	5
合計				12,857,000	22,857,000		
				$35,714,000 元			

台南市:

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	優先順序
				經常門	資本門		

108年度	1	汰換基層機關(公所社政及衛政)7年以上電腦設備	購置基層機關(公所社政及衛政)7年以上電腦設備	0	4,200,000	108年底前完成汰換基層電腦設備達106年及107年達7年以上伺服器21台	1
	2	建置區域聯防情資分享機制	建置區域聯防情資分享機制	3,286,000	0	配合行政院政策	2
	3	加強資安防禦縱深，購置資安設備	落實各項資安責任等級應辦事項(含SOC資安監控主機、網站弱掃、資安防禦縱深設備、防毒、郵件過濾、資安人力服務)、購置資安防禦縱深設備	11,354,000	13,086,000	資安責任等級要求	4
	4	研提創應用，強化資安機制	建立AD及GCB機制	0	7,000,000	配合行政院政策	3
109年度	1	汰換基層機關(公所社政及衛政)7年以上電腦設備	購置基層機關(公所社政及衛政)7年以上電腦設備	0	0	本年度無	
	2	建置區域聯防	建置區域聯防情資分享機制	3,286,000	0	配合行	1

		情資分享機制				政院政策	
	3	加強資安防禦縱深，購置資安設備	落實各項資安責任等級應辦事項(含 SOC 資安監控主機、網站弱掃、資安防禦縱深設備、防毒、郵件過濾、資安人力服務)購置資安防禦縱深設備	21,000,000		資安責任等級要求	2
	4	研提創新應用，強化資安機制	建立 AD 及 GCB 機制		0	本年度無	
合　　計				63,212,000 元			

七、 經費補助表

雲林縣：

年度	總經費	其他基金或補助款	地方政府自籌款	行政院資通安全處補助款
108	12,875,000	0	2,575,000	10,300,000
109	37,050,000	0	7,410,000	29,640,000
合計	49,925,000	0	9,985,000	39,940,000

嘉義縣：

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(配合款)	行政院資通安全處補助款
108	6,784,000	0	678,000	6,106,000
109	21,549,000	0	2,155,000	19,394,000

合計	28,333,000	0	2,833,000	25,500,000

嘉義市：

單位：新臺幣元

年度	總經費	其他基金或補助款	地方政府自籌款	行政院資通安全處補助款
108	17,000,000		5,100,000	11,900,000
109	18,714,000		5,614,200	13,099,800
合計	35,714,000		10,714,200	24,999,800

台南市：

單位:新臺幣元

年度	總經費	其他基金或補助款	地方政府自籌款	行政院資通安全處補助款
108	38,926,000	0	11,678,000	27,248,000
109	24,286,000	0	7,286,000	17,000,000
合計	63,212,000	0	18,964,000	44,248,000

八、預定進度

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
108/12	26%	12,875,000	完成第 1 批更換衛政、社政、公所電腦更換。
109/12	100%	49,925,000	完成第 2 批更換衛政、社政、公所電腦更換及資安防禦縱深，購置資安設備。

嘉義縣：

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
108/10	53%	6,784,000	108 年 10 月完成第 2 批更換衛政、社政、公所電腦更換及公所契約資安責任等級要求。
109/10	100%	28,333,000	108 年 10 月完成第 3 批更換衛政、社政、公所伺服器更換及資安責任等級要求。

嘉義市：

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
108/01	0%	0	建置區域聯防 ISAC 機制及 SOC 監控系統
108/04	14%	5,530,000	汰換資訊軟硬體設備
108/07	25%	10,095,000	採購資安設備及軟體
108/10	49%	19,895,000	資安健診及技術服務項目
109/01	53%	21,425,000	建置區域聯防 ISAC 機制及 SOC 監控系統
109/04	67%	26,955,000	採購資安設備
109/07	70%	28,495,000	建置機房雲端資源服務
109/10	100%	40,525,000	資安健診及技術服務項目

台南市：

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點

108/12	6%	4,200,000	汰換基層機關電腦設備
108/12	11%	7,486,000	建置區域聯防情資分享機制
108/12	50%	31,926,000	資安責任等級應辦事項及技術服務項目、購置資安設備
108/12	61%	38,926,000	AD 及 GCB 創新應用服務
109/12	66%	42,212,000	建置區域聯防情資分享機制
109/12	100%	63,212,000	資安健診及技術服務項目

九、預期效益

(一) 強化基層機關個人電腦作業系統安全，減少遭駭客利用 Windows XP 漏洞之風險。

(二) 執行縣市資安區域聯防，料敵機先，快速應變及即時處理，並可達成區域資安情資分享之功能。

(三) 強化網路端資安設備防禦能量，防堵或封鎖駭客入侵管道，避免公務重要資料被駭客入侵，甚至影響民眾權益。

(四) 透過創新應用，補足各縣市目前資安機制缺口，快速佈署及情資整合，強化資安體質。

(五) 利用產學資源，透過產學合作，培養資安人才。

(六) 加強使用國內資安產品，有效扶植國內資安產業發展。

十、相關聯絡資料

單位：台南市政府智慧發展中心
聯絡人：分析師李佳璋
電話分機：06-3901181
電子郵件信箱：splay@mail.tainan.gov.tw

單位：雲林縣政府計畫處資訊管理科
聯絡人：管理師羅瑞翔
電話分機：05-552-2992
電子郵件信箱：ylhg02152@mail.yunlin.gov.tw

單位：嘉義縣政府綜合規劃處資訊管理科
聯絡人姓名：技士楊忠憲
電話：05-3620123#243
電子郵件信箱：samyang@mail.cyhg.gov.tw

單位：嘉義市政府智慧科技處資通建設科
聯絡人姓名：科長蔡育勝
電話：05-2254321#769
電子郵件信箱：juijen@ems.chiayi.gov.tw

附件 8

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之分項計畫

高雄市

108年3月

高雄市政府、屏東縣政府
臺東縣政府、澎湖縣政府
前瞻基礎建設計畫

一、 計畫緣起

因應行政院 106 年 4 月 5 日核定通過之「前瞻基礎建設計畫」，其中「數位建設」子項目-「強化政府基層機關資安防護及區域聯防」須提出競爭型計畫以爭取中央補助，並考量地方政府基層機關資安防護薄弱，確有加強資安區域聯防之必要，爰結合高雄市、屏東縣、台東縣及澎湖縣等鄰近區域縣市政府及產學界共同提案以強化基層機關之資安防護以符合行政院函頒之「政府機關（構）資通安全責任等級分級作業規定」強化基層資安防護，提升基層機關之資訊服務能量、建置區域資安聯防、加強資安防禦縱深及創新服務整合並研提持續營運規劃，亦期能有助於帶動資安產業發展，特擬訂本計畫。

二、 計畫目標

因應資安問題日益嚴峻，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以及規劃 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，以發揮資安資訊分享與分析的功效，如下說明：

1.強化基層機關資安防護體質，完備機關資安基礎建設

(1)落實資通安全責任等級資安防護要求

對所轄下之機關對外服務重要系統網站及主機執行滲透測試、弱點掃瞄、資安健診等資安服務。

(2)導入政府組態基準(GCB)：建立及合適規範的一致性安全設定，以降低資訊終端設備成為駭客入侵管道的機率。

(3)配合導入 GCB，將老舊資訊設備、系統汰換：逐步汰換基層機關老舊之個人電腦及伺服器主機，以即時獲得漏洞及安全性更新等原廠服務支援，降低資安事件發生率。

(4)弱點掃瞄管理共同平台(創新應用)

透過共用弱點掃描檢測平台，使各級機關能有效掌握本身聯外服務之設備是否存在弱點，並能有效自主管理，設定排程進行掃瞄，減低人力負荷。

(5)強化縣市政府(高雄市、屏東縣、台東縣、澎湖縣)區域聯防資安縱深防禦：

A.資訊機房網路及資安設備更新升級、汰換與強化。

B.縣(市)府與基層機關 VPN 網路架構建置及導入：強化各所屬基層機關（資安等級Ｃ級及Ｃ＋級機關）資安防護縱深、提升基層機關之資安防護能量。

C.擴大資安監控（Security Operation Center，簡稱 SOC）7*24 資安監控服務機制至基層機關：協助掌控基層機關資訊安全狀態及風險等級並提供必要的技術支援，以持續性控制基層機關資安風險。

D.建立縣市與基層機關區域性 APT 持續威脅防禦機制，強化縣市與基層機關網路安全：確保所有基層機關都具備一定強度的防禦能力，在進行防禦串聯時，不會因為某一機關防禦強度不足，而影響整體防禦的能量，以期健全整體資安體質，強化資安基礎建設。

E. 充實各項資安防護措施

高雄市	屏東縣	台東縣	澎湖縣
● SSL 加解密系統 ● Web 網頁安全閘道系統 ● Web 應用程式防火牆備援機制 ● 簡化網路架構建立資安資料可視性分析	● 強化網路防禦，導入次世代防火牆及網路行為管理設備，建置 APT 防禦機制 ● 整合網路管理系統，導入網路權限管理、阻擋使用者電腦私接網路 ● 端點防護，GCB 強化端點資安基礎設定	● 強化資安防護縱深 ● 提升縣府系統及網路設備可用性 ● 強化實體監控	● 擴大 SOC 監控範圍，並導入新一代防火牆設備。提升防護層級 ● 導入 GCB 政府組態基準，強化資安基礎環境安全設定及終端防護 ● 強化資安防護縱深、提升整體資安防護能量及建立 APT 防禦監測機制

2.建立資安區域聯防監控

建立鄰近縣市資安聯防機制彙整所屬鄰近縣市之資安情資，進行綜合分析以掌握可疑惡意行為。

(1)建立區域聯防監控系統

將各機關的資安事件單收容，可對資安事件做跨機關的進階式規則分析，找出各機關的類似攻擊事件，判定駭客的攻擊趨勢與走向，達到區域聯防監控的目標。

(2)建立區域聯防情資系統

分享資安防護規則(如防火牆規則、IPS/IDS 偵測規則等)與攻擊活動訊息(如可疑郵件主旨列表、可疑連線 IP、惡意留言等)，發生大規模之網路攻擊(如勒索軟體、蠕蟲發作等)時，即時通知所屬鄰近縣市進行預防或增設阻擋規則。

(3)建立區域聯防防護規則派送系統

透過平台機關可自主管理及派送防禦阻擋規則(如:技服新公告之惡意中繼站)。

(4)擴大各縣市資安監控範圍

建置並擴大 VPN 機關，統一上網出口防護及監控；或針對區域內機關，若未有足夠防護該機關之設備，導入新聯防設備服務。本設備要能配合 ISAC 區域聯防防護規則派送系統功能，於第一時間接收到防護規則的配送。

3.建立資安事件快速應變小組及處理流程

(1)成立資安快速應變小組

發生重大資安事件時(如資料洩漏、大規模網頁置換、SPAM、中毒等)，透過資安快速應變小組，協防所屬鄰近縣市並提供資安諮詢或技術支援。

(2)資訊安全教育訓練

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，以培養各級機關資安專業人才為核心，藉由實務操作演練、持續教育訓練，厚植 機關人才資源，逐步建立資安自主作業能量。

(3)結合地區大學能量合作

培育機關所需之資通訊安全專業人才，鼓勵公私立大學校院曾受過資通安全學程訓練之學生參與前瞻計畫區域聯防規劃，體驗資通安全實務，並透過現場的訓練與操作程序，落實「學以致用」的目標，並期使民眾能有機會親身參與了解前瞻計畫資安聯防推展之目的與效益。

三、 計畫內容與實施策略

1.全面強化基層機關資安防護體質，完備機關資安基礎建設

(1)落實資通安全責任等級要求

執行方式：

- 規劃針對各級機關外部網站及伺服器主機數量，執行滲透測試及弱點掃瞄服務，並以核心資訊系統優先執行。
- 統計機關數量，執行資安健診服務。
- 預計於 107~109 年，依資通安全責任等級對 A 級、B 級、C+及 C 級機關規定，於規定期間內執行滲透測試、弱點掃瞄、及資安健診服務以提升資安防護。

(2)導入政府組態基準(GCB)：

為配合行政院要求導入政府組態基準(Government Configuration Baseline, GCB)，惟地方政府資安人力極為缺乏，導入 GCB 時，亦涉及眾多個人電腦端數量，設定繁瑣，推廣不易，須借助 AD 及管理工具及專業顧問輔導，方能大量逐步導入 GCB 一致性設定，增加資安防護。

高雄市	屏東縣	台東縣	澎湖縣
● 無 AD ● 引進 GCB 管理工具,公所導入 GCB	● 無 AD ● 引進 GCB 管理工具 ● 依規定推動資安責任等級 B 級以上機關導入，後續再配合中央期程推動 C+及 C 級機關導入	● 無 AD ● 引進 GCB 管理工具,公所導入 GCB	● 有 AD ● 公所納入 AD，布署 GCB 設定

(3)配合導入GCB政府組態基準，老舊資訊設備、系統汰換：

為配合導入GCB政府組態基準,將資安風險已高的老舊資訊設備汰換,將已終止支援的作業系統的個人電腦及電腦伺服器汰換升級，避免形成各機關整體資安防護的弱點，本區各縣市所提數各年度汰換數量如下：

機關別	伺服器數量			個人電腦數量		
	107	108	109	107	108	109
高雄市政府		—	—		1276	1350
屏東縣政府		—	—		120	—
台東縣政府		—	15		300	200
澎湖縣政府		—	5		376	350

(4)弱點掃瞄管理共同平台(創新提案)

弱點掃瞄管理為資安防護基礎措施，但由於縣市網站系統數量眾多，依資安責任等級應辦事項，須定期進行網站及系統弱點掃描，但往往地方政府及基層機關因人力、財力不足，常無法合乎規定進行網站弱點掃描及弱點修補，容易造成資安事件。

因應區域聯防計畫，擬建立跨縣市共用全自動弱點掃瞄管理平台，供本區各縣市使用，依需求可自行利用網站弱點掃描，事先掌握弱點修補，減少駭客入侵管道。

執行方式：建立一套弱點掃瞄管理共同平台，並讓本區域內的所有機關共同使用及自主管理。

平台功能：此平台將擁有以下功能。

- 網頁弱點掃瞄功能
- 主機弱點掃瞄功能
- 帳號管理功能
- 依帳號權限管控所轄主機功能
- 自主設定主機掃瞄排程
- 弱點處理/修補回報

- 弱點自動複檢
- 統計報表功能

(5)縣市資安防護縱深設備需求(縣市自提之需求設備)

2.建立資安區域聯防整合服務架構，建立鄰近縣市資安聯防機制，資安區域聯防監控規劃方向共區分五項實施要點，整體架構圖如下所示。

實施要點如下：

(1)擴大區域縣市資安監控範圍至 C+級、C 級機關，以利第一時間發現區域聯防各級機關的資安事件降低資安死角，俾利區域資安應變作為。

(2)區域聯防監控系統，以對區域內的資安威脅做整體分析。

(3)區域聯防情資系統，以圖表呈現分析區域內的資安狀況，並於資安平台呈現整體趨勢分析及資安攻擊板塊。

(4)區域聯防防護規則派送系統，機關可自主或自動化派送防護規則到機關所屬對外資安防護設備。

(5)資安聯防設備導入與建置對各機關部署聯防設備。

執行方式：

(1)區域聯防監控系統

- 以直轄市為核心規劃區域聯防監控系統，收容區域範圍內各機關資安監控之通報事件單(Event Log)，其事件單格式也必須遵循行政院資通安全處二線聯防制定之聯通規範，以利將事件單資訊一併回傳至技服中心進行二線監控。
- 對各機關通報事件進行整合，彙整安全設備日誌與做關聯式分析。
- 依照技服中心二線監控月報格式，定期產出區域資安事件統計報表

(2)區域聯防情資系統

透過情資的蒐集、交換及分析，了解本區域之資安威脅與攻擊事件資訊，並提供分析結果與對策，針對可能之威脅進行有效預防措施；此外，並能與 N-ISAC 平台進行情資交流，強化情資分享與協調聯防機制，透過分享資安相關情資與分析報告，以利決策者與資安防護人員有效因應資安事件。

(3)區域聯防防護規則派送系統

以直轄市為核心，規劃區域聯防防護規則派送系統。當有新惡意中繼站或新攻擊模式出現，經由情資系統分析確認後，即可對受管控之資安設備進行防護規則派送。

(4)擴大各縣市資安監控範圍

- A 級及 B 級機關部分：

  ■ 依機關流量狀況及監控需求，依循共同供應契約之資安服務規格進行規劃及執行監控作業。

- C+級及 C 級機關部分：

  ■ 建置 VPN 機制，經由單一出口統一上網防護。
  ■ 區公所及部份府外獨立小型單位資訊人力及資訊預算不充

足易造成安全防護漏洞，容易成為網路不法分子攻擊弱點。透過網路架構升級調整將部份區公所及部份府外獨立小型單位納入縣(市)府現有 GSN VPN。透過縣(市)資源向上集中，資安設備統一控管減少多個網際網路出口維護不易及控管不易缺點。

- 高雄市、台東縣及澎湖縣統一以VPN收容各所屬基層機關，由出口端資安設備統一防護，由上層統一收容 log 進行監控，達到區域聯防阻擋效果。
- 屏東縣政府規劃針對縣府所屬機關擴大現有 SOC 監控範圍，以達到提升機關資安防護強度及區域聯防阻擋效果。

3.建立資安事件快速應變小組及處理流程

建立資安快速應變小組，協防所屬鄰近縣市之資安技術支援並負責日常維運、資安情資交換運作、及派送阻擋規則以及對應各級機關資安人員建立三級資安風險應變制度及專家顧問諮詢

(1)成立資安快速應變小組

將於區域聯防中心內成立【資安快速應變小組】，其中包含四個分組，分別是【SOC/ISAC 平台維護組】、【二線 SOC 分析監控組】、【ISAC 組(事件調查與鑑識)】、【產學合作訓練組】、與【產學合作研究研發組】，以協防所屬鄰近縣市在重大資安事件發生後執行緊急應變、入侵管道定位、受影響範圍評估及回復受駭系統。

- 各分組職能說明如下：

【SOC/ISAC 平台維護組】負責情資發布及事件通報與規則派送。

【二線 SOC 分析監控組】負責收集外部及所屬機關情資進行情資分析。

【ISAC 組(事件調查與鑑識)】負責資安應變程序及情資咨詢，

【產學合作訓練組】負責辦理產學合作實習教育訓練及協調實習人員支援 ISAC 組執行資安事件調查與鑑識。

【產學合作研究研發組】負責與大專院校合作，推動資訊安全合作計劃。

(2)資訊安全教育訓練

課程內容與預期目標

針對機關資安人員實施教育訓練，目的在幫助資安人員瞭解最新的資安技術以強化資訊安全防護能力。此外，為了能使各機關資安防護系統管理者熟悉監控設備相關系統操作，規劃提供相關系統功能及運作機制之教育訓練課程，目的在協助各級機關資安人員迅速熟悉相關資安監控系統平台功能操作及運作機制，更能有效率地控管各式資安事件。課程內容設計將以提升學員參與程度，並提升講師與學員之互動程度為主要考量，藉以提升學習效果。

教育訓練方式

教育訓練分為「資安情資監控教育訓練」與「資安專業訓練」，前者於維運期間，每年度安排機關平台操作管理相關之教育訓練；並安排各課程一次性之外部資安專業訓練，其目的在於提供強化資安工作、提升資安管理所需之專業認證教育訓練。

「資安情資監控教育訓練」，專案執行期間，每年規劃 30 小時訓練課程，內容將以當年最新資安相關技術與系統操作管理為主。

「資安專業訓練」為了能使機關內相關資安監控人員及系統管

理者熟悉本案建置之相關系統操作，進行相關系統功能及運作機制之教育訓練課程，目的在協助相關系統管理者及資安監控人員迅速熟悉相關系統技術及運作機制，更能有效率地控管各式資安事件並將安排由原廠授權之技術教育訓練單位施予訓練。

(3)結合地區大學能量合作

資安服務與技術研發為國家之重點發展項目，因應未來國家資安產業擴展須持續補充資訊安全人力之需求，且因資訊安全技術及駭客攻擊手法的演進日新月異，技術門檻高，資訊安全人才之招募與養成不易，故藉由本專案與學術機構合作，透過產業實習計畫的方式，及早尋找並培養有潛力之資安人才，以壯大國家之資安能量。

A.有關資安產學合作之執行方式，規劃為產學合作實習

- 例如透過與中華民國資訊安全協會及大專院校合作，於每年度暑期提供實習名額。
- 實習工作內容：

  i. 縣市府資安區域聯防相關作業：包含弱點掃瞄、SOC 日常監控、機關資安事件協同處理、惡意程式行為分析、網路及資安設備維護、資訊安全技術文件撰寫等。
  ii. 區域聯防之資安監控中心：包含資安攻擊趨勢分析、滲透測試工具實作、惡意檔案分析、移動終端攻擊與防護技術分析等。

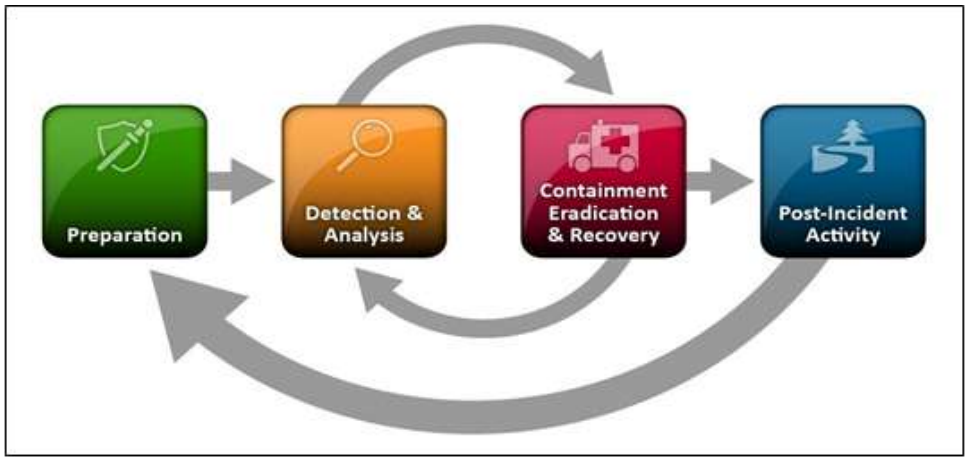
(4)資安事件應變流程

如遇「國家資通安全通報應變作業綱要」之「4」、「3」級事件(故)如:惡意(程式、網路)攻擊、非經授權之存取、資料遭竄改或竊取、資訊服務遭攻擊中斷服務病毒蠕蟲爆發之高風險事件。資安事件應變小組將於事件(故)通報或事件(故)發生 60 分鐘內依據提供者需求採電話、傳真、手機簡訊、電子郵件等方式，將資訊安全事件(故)通報本機關（構）資訊安全事件聯絡人員，整個處理流程如下：

圖、資安快速應變小組事件處理流程

(5) 資安鑑識分析處理流程

本機關將參考美國國家標準與技術研究院(NIST)的【Computer Security Incident Handling Guide (SP800-61r2)】建立事件故處理流程，共可分為四個主要階段：【準備(Preparation)】、【檢測和分析(Detection & Analysis)】、【遏制根除和復原(Containment Eradication & Recovery)】與【事件後活動(Post-Incident Activity)】。



參考來源: NIST SP800-61r2 p.21

- 準備階段：所謂事件【準備】之目的，一方面為了在事件發生時建立聯繫、確定程序與收集資安事件資料，以利在事件發生時節省處理時間之外；另一方面也是為了日後相同事件發生前，

能夠提前收到告警資訊，以預做防範。

- 檢測和分析階段：【檢測】之目的在於協助應變小組判斷事件類別及其影響範圍，以採取有效的緊急應變措施。【分析】之目的，在判斷資安事件等級，並指派合適的人員進行處理與溝通協調。
- 遏制根除和復原階段：【遏制】之目的是限制資安事件的影響範圍，某些事件會造成大規模破壞及快速擴散，例如零時差漏洞網路蠕蟲攻擊，在造成更嚴重破壞前，應設法限制其影響程度。【根除】是指清除事件根因，例如修補作業系統安全性漏洞。【復原】目的在於恢復系統的正常操作，須進行系統復原前安全評估，以確保受駭系統及其相關元件已能夠安全正常使用。
- 事件後活動階段：【事件後活動】之目的在於瞭解為何事件會發生？如何防止事件重複發生？應執行的改善措施？以及後續的監控與告警措施是否須調整精進？讓惡意行為在活動初期就能夠被發現。
- 分析追蹤過程中，發現需提升風險等級時，應依事件(故)升級處理之機制，迅速回應處理。
- 資安事件(故)確立後將立即進行蒐證，蒐證內容與報告內容將能透過資安事件(故)資料交換協定與二線 SOC、區域 ISAC 達到資訊交流並透過 tructured Threat Information eXpression(STIX)與 Trusted Automated eXchange of Indicator Information(TAXII)，進行資安事件傳輸格式與傳輸架構，以完備 SOC 及 ISAC 間的協同合作。
- 資安事件(故)各項資訊蒐集與鑑識之電子記錄、書面資料等各種形式的資訊，均應至少保留 1 年以供後續備查分析使用，並製成案例宣導(去識別化)以利後續強化區域資安人員資安管理作為。

四、 實施範圍

本計劃範圍包含高雄市政府、臺東縣政府、屏東縣政府、及澎湖縣政府，及其轄下戶政、衛政、社政、基層公所等機關。

五、 計畫期程

本計畫自 107 年 1 月起至 109 年止，共計 3 年，並依照行政院補助計劃核可費用實施。

計畫名稱	107 年	108 年	109 年
一、高雄市政府**細部計畫**			
(一)資安區域聯防			
(二)子項計畫-汰換基層機關資訊設備			
(三)子項計畫-強化縱深資安防護			
二、屏東縣政府**細部計畫**			
(一)子項計畫-區域聯防			
(二)子項計畫-汰換基層機關資訊設備			
(三)子項計畫-強化資安縱深防護			
(四)子項計畫-創新 e 化服務			
三、台東縣政府**細部計畫**			
(一)子項計畫-汰換基層機關資訊設備			
(二)子項計畫-強化資安縱深防護			
(三)子項計畫-創新 e 化服務			
四、澎湖縣政府**細部計畫**			
(一)子項計畫-汰換基層機關資訊設備			
(二)子項計畫-強化資安縱深防護			
(三)子項計畫-資料中心資訊安全防護計畫			
(四)子項計畫-創新 e 化服務			

六、 關鍵績效指標及年度目標值

資安區域聯防關鍵績效指標：

項次	主要績效指標	目標	權重	如何完成預期目標
1	建立自動弱點掃描平台，擴大使用機關	達到資通安全責任等級要求100%	10%	1. 統計機關網站及外部伺服器主機數量，依資通安全責任等級要求定期執行資安服務，如滲透測試、弱點掃描、資安健診。
2	擴大資安監控範圍至各級機關	1.K-ISAC 涵蓋高雄、屏東、澎湖、臺東，涵蓋率 100%。 2.各縣市所屬涵蓋率：高雄95%以上、屏東(不含區公所及衛所)100%、澎湖95%以上、臺東50%以上。	15%	1.確實依據區域聯防內各級機關納入各級資安監控範圍
3	區域聯防監控系統	區域聯防內各級機關資安監控事件單完成回傳，並能進行二線分析	10%	1. 要求各級機關所使用之SOC 服務及平台於時限內完成回傳設定 2. 針對回傳之事件單進行定義統計及趨勢分析
4	區域聯防情資系統	以圖表呈現分析區域內的資安狀況，並於資安平台呈現整體趨勢分析及資安攻擊板塊	20%	完成界接內外部情資系統，並能以圖表方式呈現情資安分析，以區分各級機關所需之情資與資安攻擊
5	區域聯防防護規則派送系統	機關可自主或自動化派送防護規則到機關	10%	1. 完成區域聯防防護規則與聯防設備之連動設定。 2. 依據機關需求可自動或被

		所屬對外資安防護設備。		動遠端派送防護規則導入。
6	資安聯防設備導入與建置	完成各級機關資安聯防設備導入	10%	1. 完成機關聯外資安防護設備需求調查。 2. 依據機關連外資安防護設備之區域聯防防護規則連動。
7	資安事件應變處理	依行政院國家資通安全會報技術服務中心要求，於規定時間內完成資安事件處理	10%	1. 於資安事件通報後，於行政院國家資通安全會報技術服務中心規定時間內完成資安通報及處理。
8	資訊安全教育訓練	每年提供30個小時教育訓練時數	5%	1. 每年度第一季公布課程實行規劃,並於第二季~第三季完成課程 2. 每年度依據課程規劃，通知各級機關選訓適當人員進行課程
9	結合地區大學能量合作	每年提供產學合或實習名額	10%	1. 預計每年度於當年學年度開學前與合作之學校規劃產學合作實行計畫，編列實習名額，並請學校推薦適合之學生面試及選訓。

七、 持續營運評估

為持續加強資安防護，在計畫期程結束後，各項工作會持續由各縣市編列經費來永續經營。

1.區域聯防與情資交換部分，因屬共同使用之系統，規劃採費用平均分攤方式。由各縣市府一起編列後續維運經費，讓相關資訊系統得以持續進行，並逐年檢討成效。

2.資安教育訓練部分將持續協請資安廠商及大專院校，共同持續舉辦

資安論壇，並與區域聯防中心進行意見交流。產學合作部分持續與中華民國資訊安全協會合作，針對區域內大學，持續提供實習名額，並建立資安事件處理研究計劃。除了讓資訊相關科系學生得以有實際的產業參與機會，也讓學生得以從過去的資安事件故，研發出可快速分析定位工具。

3.防護縱深強化部分則會持續汰換老舊電腦，以及投入經費在資安設備上的維護及訓練。資通安全責任等級之要求(如：資安監控、滲透測試、弱點掃瞄、資安健診)也會由各機關持續編列經費進行，以持續強化資安防護體質。

八、 經費明細概算

(一)資安區域聯防

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		
108	1	區域聯防主計畫： 資通安全責任等級要求資安防護要求	達到行政院資通安全責任等級資安防護要求	2,500,000	0	1.完成對外服務重要系統網站及主機執行滲透測試、弱點掃瞄、資安健診等責任等級要求。 2.韌體更新至最新版。	1
	2	區域聯防主計畫： 區域聯防監控系統	於本區域建置區域聯防監控系統，供本區域內轄下所有機關回傳資安事件	4,500,000	0	持續區域聯防監控系統維運	
	3	區域聯防主計畫： 區域聯防情資系統	於本區域建置區域聯防情資系統	4,500,000	0	持續區域聯防情資系統維運	
	4	區域聯防主計畫： 資訊安全教育訓練與產學合作	1.講師課程費及外訓課程費用 2. 實習人員月薪及勞健保費用	250,000	0	每年提供學生實務見習名額。(高雄市)	
	5	區域聯防主計畫： 擴大資安監控範圍	1. 因應 VPN 收容各公所，擴大資安監控容量。 2.所屬 B、C 及 C+級機關納入資安監控範圍。	1,296,000	0	增加 1 單位高流量資安監控	
108	6	子計畫 1-2-強化資安縱深防護： 建置入侵偵測防禦系統（NGIPS）	四維行政中心與鳳山行政中心建置專業入侵偵測防禦系統設備	0	5,000,000	建置雙行政中心專業入侵偵測防禦系統(NGIPS)設備並將訊息匯整與 SOC 平台結合	3

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		
	7	子計畫 1-2-強化資安縱深防護：GCB 建置	建立 GCB 組態基準調整與佈署、干擾組態排除	2,000,000	0	佈署 2000 個端點	4
	8	子計畫 1-2-強化資安縱深防護：VPN 網路架構升級調整	提升 GSN VPN 線路頻寬	1,180,000	0	提升四維行政中心 GSN VPN 線路至 300M/300M 及鳳山行政中心 GSN VPN 線路至 150M/150M	6
			提升原高雄市區域內公所及收容外部小型單位 GSN VPN 線路頻寬	0	2,100,000	1.提升原高雄市 11 個區公所 GSN VPN 頻寬並收容 31 個外部小型單位至 GSN VPN。 2.佈設 11 個公所及 31 個外部小型單位 VPN 端交換器	
	9	子計畫 1-2-強化資安縱深防護：SSL 加解密系統	建置雙行政中心 SSL 加解密系統設備	0	3,500,000	建置 SSL 加解密系統設備，提供網路可視度提升，配合國家發展委員會要求，政府機關重要對外服務網站應於 107 年 12 月底前完成使用 HTTPS 傳輸協定	8
	10	子計畫 1-2-強化資安縱深防護：Web 網頁安全閘道系統	建置雙行政中心 Web 網頁安全閘道系統設備	0	6,500,000	建置 Web 網頁安全閘道系統設備使達到建立統一出口閘道	13
	11	子計畫 1-2-強化資安縱深防護：建置智慧型流量管理平台	1.資安設備達到 Bypass 機制，AA 負載平衡機制 2.實體機及虛擬機流量收集至 SOC 平台	0	6,000,000	建置雙個行政中心智慧型流量設備，建立完善的智慧型流量管理平台，原其他資安設備之 HA 備援機制提升為 AA 備援機制，達成完善資安防護效果	14

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		
	12	子計畫 1-2-強化資安縱深防護： 端點進階持續性滲透攻擊防護系統	導入 APT 端點軟體佈署至端點 PC 並建立平台並與 SOC 整合	3,580,000		佈署 1500 個端點(3 年)並 APT 訊息與 SOC 整合	12
	13	子計畫 1-2-強化資安縱深防護：（併入區域聯防主計畫執行） 建置資安聯防設備管理平台	配合區域聯防管理及本府 ISMS 規定，將相關資安申請表單及後續處理作業以系統進行管控及設定	1,908,000		完成資安聯防設備管理平台建置	9
108	14	子計畫 1-1 汰換基層機關資訊設備： 汰換個人電腦	汰換 1350 臺 7 年以上 XP 個人電腦	0	31,900,000	汰換 1276 臺(50%)個人電腦	10
109	1	區域聯防主計畫： 資通安全責任等級要求資安防護要求	達到行政院資通安全責任等級資安防護要求	2,500,000	0	1.機關完成對外服務重要系統網站及主機執行滲透測試、弱點掃瞄、資安健診等責任等級要求。 2.完成弱點掃描共用平台租賃發包。	2
	2	區域聯防主計畫： 區域聯防監控系統	於本區域建置區域聯防監控系統，供本區域內轄下所有機關回傳資安事件	4,500,000	0	完成租賃維運區域聯防監控系統	
	3	區域聯防主計畫： 區域聯防情資系統	於本區域建置區域聯防情資系統	4,500,000	0	完成租賃維運區域聯防情資系統	
	4	區域聯防主計畫： 資訊安全教育訓練與產學合作	1.講師課程費及外訓課程費用 2.實習人員月薪及勞健保費用	250,000	0	每年提供學生實務見習名額。(高雄市)	

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		
	5	區域聯防主計畫： 擴大資安監控範圍	1.因應 VPN 收容各公所，擴大資安監控容量。 2.所屬 B、C 及 C+級機關納入資安監控範圍。	1,296,000	0	增加 1 單位高流量資安監控服務	
109	6	子計畫 1-2-強化資安縱深防護： 建置 Web 應用程式防火牆	增設四維行政中心及鳳山行政中心 Web 應用程式防火牆	0	3,000,000	增設雙行政中心 Web 應用程式防火牆	11
	7	子計畫 1-2-強化資安縱深防護： GCB 建置	建立 GCB 組態基準調整與佈署、干擾組態排除	3,000,000	0	佈署 3000 個端點	5
	8	子計畫 1-2-強化資安縱深防護： VPN 網路架構升級調整	提升 GSN VPN 線路頻寬	1,180,000	0	提升四維行政中心 GSN VPN 線路至 300M/300M 及鳳山行政中心 GSN VPN 線路至 150M/150M	7
			收容外部小型單位 GSN VPN 線路頻寬		1,550,000	收容 31 個外部小型單位至 GSN VPN 並建置 31 個外部小型單位 VPN 端交換器	
	9	子計畫 1-2-強化資安縱深防護： 端點進階持續性滲透攻擊防護系統	導入 APT 端點軟體佈署至端點 PC 並建立平台並與 SOC 整合	3,580,000		佈署 1500 個端點(3 年)並 APT 訊息與 SOC 整合	15
	10	子計畫 1-2-強化資安縱深防護： 建置資安聯防設備管理平台	配合區域聯防管理及本府 ISMS 規定，將相關資安申請表單及後續處理作業以系統進行管控及設定	1,398,000	1,166,000	強化資安聯防設備管理平台功能及持續維運	14
109	11	子計畫 1-1 汰換基層機關資訊設備：	汰換 1350 臺 7 年以上 XP 個人電腦	0	33,570,000	汰換 1350 臺(100%)個人電腦	13

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		
		汰換個人電腦					
合　　計				138,204,000 元			

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		
108	1	(一)子項計畫-區域聯防： 針對前瞻計畫已協助導入 SOC 及納入本區資安區域聯防的機關，維持機制運行(107 年已納入 3 個機關)	提供 SOC 監控服務 (經費估計:1 個中流量、2 個低流量)	2,193,000		維持 SOC 監控服務正常運行	5
	2	(一)子項計畫-區域聯防： 協助本縣機關導入 SOC 及納入本區資安區域聯防(108 年預計再納入 3 個機關)	於各機關設定自動化防禦機制	0		完成於各機關設定防護規則自動派送機制	6
			提供 SOC 監控服務 (經費估計:3 個低流量)	1,833,000		完成 SOC 監控服務建置及維護正常運行	
	3	(一)子項計畫-區域聯防： 提供各機關資安諮詢服務、事件列管機制、	建立資安諮詢服務窗口及資安事件列管機制	1,500,000		建立並維持 SOC 通知重大事件列管追蹤機制 建立 5*8 資安諮詢與輔導服務電話專線及運作機制	4

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		
		教育訓練課程	規劃及辦理資安教育訓練4場次	100,000		完成辦理資安教育訓練	
	4	(一)子項計畫-區域聯防： 縣內機關共用系統之資安檢測	辦理應辦之滲透測試、資安健診、網站/系統弱點掃描、電子郵件演練、通報演練或ISMS…等資安檢測	0		完成應辦之滲透測試、資安健診、網站/系統弱點掃描、電子郵件演練、通報演練等	13
	5	(一)子項計畫-區域聯防： 產學合作培育在地資安人才	與地區大專院校合作	60,000		完成與地區大專院校合作事項	7
	6	(二)子項計畫-汰換基層機關資訊設備： 汰換縣府老舊不堪使用的電腦(符合超過7年且CPU效能不足)	汰換120台電腦		3,000,000	該機關老舊不堪使用的個人電腦數量佔總比率10%以下	1
	7	(二)子項計畫-汰換基層機關資訊設備： 升級縣府採用已不支援作業系統的電腦(Vista、Windows Server 2003以前的作業系統)	取得120套最新版作業系統		720,000	該機關使用Windows Vista以前作業系統的個人電腦數量佔總比率10%以下	2

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		
	8	(三)子項計畫-強化資安縱深防護：網路防禦與資安管理	建立本府廣域網路頻寬負載平衡容錯機制		3,000,000	廣域網路頻寬負載平衡容錯機制	3
	9	(三)子項計畫-強化資安縱深防護：端點防護	導入 GCB 強化端點資安基礎設定(包含本府及財稅局)	2,083,000		維護電腦 GCB 派送及定期查核	12
	10	(三)子項計畫-強化資安縱深防護：資安產業與學研技術合作	討論各項資訊安全相關議題及最新發展趨勢	20,000		定期召開機關與產學界聯合會議	8
	11	(四)子項計畫-創新 e 化服務：辦理 open source 教育訓練及說明會	1. 舉辦 open source 軟體應用訓練及相關說明會，供府內外機關含縣立學校同仁瞭解及使用 2. 辦理 open source 文件編輯軟體操作課程 3. 提供顧問諮詢及技術支援，解決同使用相關問題	100,000		辦理 open source 相關教育訓練計 7 場	9
	12	(四)子項計畫-創新 e 化服務：推動全縣電子公文交換之附件以 ODF 等開放格式為主	1. 建立本縣公文管理資訊系統之線上 ODF 轉檔、轉檔後即時預覽/編輯等相關功能，協助同仁透過系統即可完成轉檔。		624,000	本府各局處、地/戶政事務所、警察分局、鄉鎮市衛生所、公所及代表會之公文附件	10

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		
			2. 建立本縣公文管理資訊系統良好的系統流程介面，引導同仁將公文附件採用 ODF 檔案等開放格式。			文件檔案之格式為 ODF 或其他開放格式，佔比率達 45%以上	
	13	(四)子項計畫-創新 e 化服務： 推動擴大本府即時通訊平台使用對象	1. 強化本府即時通訊平台功能，建立機關與同仁需求或已慣用的資訊交換相關功能。 2. 擴充本府即時通訊平台使用人數授權，推動本府所有同仁及跨機關使用者導入使用本府即時通訊平台互相聯繫。		900,000	新增 500 個使用者導入使用本府即時通訊平台	11
109	1	(一)子項計畫-區域聯防： 針對前瞻計畫已協助導入 SOC 及納入本區資安區域聯防的機關，維持機制運行(107 年及 108 年共納入 6 個機關)	提供 SOC 監控服務 (經費估計:1 個中流量、5 個低流量)	4,026,000		維持 SOC 監控服務正常運行	2
	2	(一)子項計畫-區域聯防： 提供各機關資安諮詢服務、事件列管機制、教育訓練課程	建立資安諮詢服務窗口及資安事件列管機制	1,500,000		建立並維持 SOC 通知重大資安事件列管追蹤機制 建立 5*8 資安諮詢與輔導服務電話專線及運作機制	1
			規劃及辦理資安教育訓練 4 場次	100,000		完成辦理資安教育訓練	

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		
	3	(一)子項計畫-區域聯防： 縣內機關共用系統之資安檢測	辦理應辦之滲透測試、資安健診、網站/系統弱點掃描、電子郵件演練、通報演練或ISMS…等資安檢測	0		完成應辦之滲透測試、資安健診、網站/系統弱點掃描、電子郵件演練、通報演練等	7
	4	(一)子項計畫-區域聯防： 產學合作培育在地資安人才	與地區大專院校合作	60,000		完成與地區大專院校合作事項	3
	6	(三)子項計畫-強化資安縱深防護： 端點防護	導入 GCB 強化端點資安基礎設定(包含本府及財稅局，預計再納入消防局、衛生局、環境保護局)	3,316,000	200,000	維護電腦 GCB 派送及定期查核	6
	7	(三)子項計畫-強化資安縱深防護： 資安產業與學研技術合作	討論各項資訊安全相關議題及最新發展趨勢	20,000		定期召開機關與產學界聯合會議	4
	8	(四)子項計畫-創新 e 化服務： 辦理 open source 教育訓練及說明會	1. 舉辦 open source 軟體應用訓練及相關說明會，供府內外機關含縣立學校同仁瞭解及使用 2. 辦理 open source 文件編輯軟體操作課程 3. 提供顧問諮詢及技術支援，解決同使用相關問題	200,000		辦理 open source 相關教育訓練計 15 場	5
合　　計				25,555,000 元			

台東縣政府

108	1-1	強化資安縱深防護-強化資安防護縱深	1. 收容公所線路至本府 VPN 2. 建置基層機關 VPN 網路架構環境需要配置之 Router 或 Firewall 設備		2,100,000	納管公所網路至本府資安設備監控	1
	1-2		提升對外頻寬	400,000		確保與公所間線路暢通	2
	1-3		購置日誌儲存、分析設備		2,250,000	符合數位鑑識要求	6
	1-4		防火牆效能提升		1,500,000	確保可負擔本府及基層公所流量	3
	1-7		建置資訊設備監控系統		420,000	掌握府內設備狀況及連線情形，有問題可即時告警	7
	1-8		配合收納基層機關流量所需，擴充更新本府網路架構		1,230,000		5
	2-1	強化資安縱深防護-執行資安責任等級應辦事項	國際資安專業證照之課程及證照取得	210,000		取得國際資安專業證照	4
	2-2		SOC 監控	2,434,000		將基層公所納入 SOC 防護	8
	3	強化資安縱深防護-資訊安全教育訓練	講師課程費及外訓課程費用	300,000		取得資安相關訓練證明或證照	10
	4	強化資安縱深防	實習人員月薪及勞健保費用	100,000		至少培養 2 名學生參與資安	11

		護-產學合作經費				實習	
	5-1	汰換基層機關資訊設備-汰換個人電腦	汰換基層單位 300 台老舊個人電腦		7,500,000	汰換 60%本縣基層單位老舊個人電腦	9
109	1-1	強化資安縱深防護-強化資安防護縱深	1. 收容公所線路至本府 VPN 2. 建置基層機關 VPN 網路架構環境需要配置之 Router 或 Firewall 設備		2,114,000	納管公所網路至本府資安設備監控	1
	1-2		提升對外頻寬	500,000		確保與公所間線路暢通	2
	1-3		更新 WAF 及 UTM 特徵碼	1,200,000		即時防護最新威脅	4
	1-4		購置資安事件管理系統	3,000,000		將資安事件處理自動化，即時防護資安攻擊	18
	1-5		強化電子郵件防護機制		2,500,000	避免惡意電子郵件	16
	1-6		購置虛擬主機效能流量監控分析軟體		1,500,000	分析監控虛擬主機流量	19
	1-7		擴充防火牆及 WAF 效能		3,500,000	確保可負擔本府及基層公所流量	3
	1-8		購置惡意中繼站防護閘道器		1,980,000	即時更新惡意中繼站位址	17
	2-1	強化資安縱深防護-執行資安責任	本府 ISMS 導入及認證	1,000,000		至少 1 個系統導入 ISMS 認證	5
	2-2		SOC 監控	2,644,000		將基層公所納入 SOC 防護	5

	2-3	等級應辦事項	網站弱點掃描，本府之系統滲透測試	875,000		本府及公所 20 個網站完成弱掃	5
	2-4		資安內稽及對所屬機關之訪視	200,000		建立基層單位正確資安觀念	5
	2-5		本府及公所 GCB 導入	2,100,000		輔導各關機導入 GCB	5
	2-6		國際資安專業證照之課程及證照取得	500,000		取得國際資安專業證照	5
	2-7		資安健診	2,000,000		檢視基層公所資安設定	5
	3	強化資安縱深防護-資訊安全教育訓練	講師課程費及外訓課程費用	500,000		取得資安相關訓練證明或證照	14
	4	強化資安縱深防護-產學合作經費	實習人員月薪及勞健保費用	200,000		至少培養 2 名學生參與資安實習	15
	5-1	汰換基層機關資訊設備-汰換個人電腦	汰換基層單位 200 台老舊個人電腦		5,000,000	汰換 40%本縣基層單位老舊個人電腦	12
	5-2	汰換基層機關資訊設備-汰換伺服主機	汰換基層單位 15 台老舊伺服主機		3,300,000	汰換 60%本縣基層單位老舊伺服主機	12

	6-1	e 化創新便民服務-推廣 ODF 說明會(含規劃、場地佈置、雜支等)	辦理 1 場推廣 ODF 說明會	20,000		辦理 1 場推廣 ODF 說明會	20
	6-2	e 化創新便民服務-推廣 ODF 教育訓練(含規劃、教材、場地借用、雜支)	辦理 5 場推廣 ODF 教育訓練	150,000		辦理 5 場推廣 ODF 教育訓練	20
合　　計				53,227,000 元			

澎湖縣政府

年度	項次	計畫名稱	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		
108	1	(一)子項計畫-資訊設備資安防護及效能提升改善計畫	汰換個人電腦	預計汰換7年以上個人電腦376臺		9,400,000	汰換7年以上個人電腦比例達52%以上	2
108	1	(二)子項計畫-強化基層機關資安防護縱深能力計畫	本府防火牆升級汰換	汰換原有對外之第四層防火牆（使用年限屆滿7年），以提升防火牆網路控管流量及至具第七層應用層功能，並建立防火牆之容錯機制，集中控管網路行為		6,230,000	有效提升防火牆應用防護層級，設備正常服務可用率達99.5%以上	1
108	2	(二)子項計畫-強化基層機關資安防護縱深能力計畫	基層機關VPN網路架構電路、設備租賃及技術支援服務	1.租用GSN VPN乙太固接專線（150M）2條 2.租用基層機關VPN網路架構環境需要配置之Router或Firewall設備 3.提供網路技術支援服務	2,097,000		至少30個基層機關納入VPN網路架構	3

年度	項次	計畫名稱	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		
108	3	(二)子項計畫-強化基層機關資安防護縱深能力計畫	將縣府所屬機關及鄉市公所資安等級C級及C＋級機關納入縣府SOC（Security Operation Center）7*24資訊安全監控及安全檢測委外服務	108年度預計辦理本府及基層機關SOC資訊安全監控委外服務：包括監控管理、網站安全性弱點檢測等，以協助掌控基層機關資訊安全狀態及風險等級並提供必要的技術支援，持續性控制基層機關資安風險	600,000		1.至少30個基層機關納入7*24資訊安全監控及安全檢測委外服務 2.至少15個網站辦理網站安全弱點檢測 3.至少3個站臺辦理系統滲透測試	6
108	4	(二)子項計畫-強化基層機關資安防護縱深能力計畫	本府及基層機關導入政府組態基準(GCB)	預計導入政府組態基準GCB管理系統及分散式弱點管理系統		1,300,000	至少30個基層機關導入政府組態基準(GCB)及分散式弱點管理系統	4
108	5	(二)子項計畫-強化基層機關資	基層機關導入AD帳號目錄	協助基層機關建立AD帳號目錄服務系統與環境建置，強化		2,200,000	至少15個基層機關導入AD帳號目錄服務系統	5

年度	項次	計畫名稱	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		
		安防護縱深能力計畫	服務系統與環境建置	端點使用權限控管，強化資安基礎作為				
108	5	(二)子項計畫-強化基層機關資安防護縱深能力計畫	與大專院校資訊相關系所合作，提供學生實務見習機會	提供資訊相關系所學生實務運作環境與機會，以強化離島地區資安防護及資安人才能量	303,000		每年至少提供 12 人次/月的學生實務見習機會	12
108	1	(三)子項計畫-資料中心資訊安全防護計畫	強化雲端資料中心資料安全性防護機制	1.雙機房骨幹網路交換器升級及建立完整備援機制 2.將伺服器群(Server Farm)獨立一個網段，與內部使用者區隔，並於共構機房建置伺服器群 10G 交換器高可用性(Active - Active)，避免單點失效		3,093,000	1.完成雙機房骨幹網路交換器升級及備援機制 2.完成伺服器群(Server Farm)獨立網段並提升傳輸速度至 10G 環境	13
109	1	(一)子項計畫-資訊設備資安防護及效能提升改	汰換個人電腦	預計汰換 7 年以上個人電腦 350 臺		8,750,000	汰換 7 年以上個人電腦比例達 100%	9

年度	項次	計畫名稱	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		
		善計畫						
109	2	(一)子項計畫-資訊設備資安防護及效能提升改善計畫	汰換伺服器主機	預計汰換7年以上伺服器主機5臺		1,000,000	汰換7年以上伺服器主機比例達50%	14
109	1	(二)子項計畫-強化基層機關資安防護縱深能力計畫	將縣府所屬機關及鄉市公所資安等級C級及C＋級機關納入縣府SOC（Security Operation Center）7*24資訊安全監控及安全檢測委外服務	109年度預計辦理本府及基層機關SOC資訊安全監控委外服務：包括監控管理、網站安全性弱點檢測、系統滲透測試、資安健診等，以協助掌控基層機關資訊安全狀態及風險等級並提供必要的技術支援，持續性控制基層機關資安風險。	5,000,000		1.至少30個基層機關納入7*24資訊安全監控及安全檢測委外服務 2.至少15個網站辦理網站安全弱點檢測 3.至少3個站臺辦理系統滲透測試 4.至少500臺個人電腦辦理資安健診工作	10
109	2	(二)子項計畫-	基層機關VPN	1.租用GSN VPN乙太固接專線	2,220,000		至少30個基層機關納入	7

年度	項次	計畫名稱	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		
		強化基層機關資安防護縱深能力計畫	網路架構電路、設備租賃及技術支援服務	（150M）2 條。 2.租用基層機關 VPN 網路架構環境需要配置之 Router 或 Firewall 設備。 3.提供網路技術支援服務。			VPN 網路架構	
109	3	(二)子項計畫-強化基層機關資安防護縱深能力計畫	基層機關政府組態基準(GCB)及 AD 帳號目錄服務系統維運服務	維持導入政府組態基準 GCB 管理系統及分散式弱點管理系統及 AD 帳號目錄服務系統之基層機關正常運作		2,000,000	至少維持 30 個基層機關政府組態基準(GCB)持續運作	11
109	4	(二)子項計畫-強化基層機關資安防護縱深能力計畫	導入 APT 偵測與防禦機制	1.建立網路威脅分析感知機制（DDI） 2.建立社交工程攻擊防禦機制（DDEI） 3.重要主機目標式攻擊防禦系統 4.防毒軟體使用授權購置		6,394,000	至少 30 個機關導入 APT 偵測與防禦機制	8

年度	項次	計畫名稱	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		
109	5	(二)子項計畫-強化基層機關資安防護縱深能力計畫	與大專院校資訊相關系所合作，提供學生實務見習機會	提供資訊相關系所學生實務運作環境與機會，以強化離島地區資安防護及資安人才能量	303,000		每年至少提供 12 人次/月的學生實務見習機會	15
109	1	(三)子項計畫-資料中心資訊安全防護計畫	異地資料儲存自動化	1 具備異地資料儲存規劃提供資料重覆刪除功能 2. 減少備份資料傳輸量 3. 節省資料傳輸頻寬及時間		2,100,000	減少備份資料量傳輸至少 20%	16
109	2	(三)子項計畫-資料中心資訊安全防護計畫	資料儲存安全防護機制之建置	在異地安裝虛擬機與資料儲存系統，利用來源端虛擬機資料重複刪除技術，將資料持續性地抄寫至異地虛擬機，因府內虛擬機系統眾多，本階段先以部分重要主機抄寫為階段目標，達成虛擬機異地備援機制。		4,200,000	完成異地備援中心基本機制建置	17
合　計					57,190,000 元			

九、 經費補助表

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
108	76,714,000		23,014,200	53,699,800
109	61,490,000		18,447,000	43,043,000
小計	138,204,000		41,461,200	96,742,800

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
108	16,133,000		1,613,300	14,519,700
109	9,422,000		942,200	8,479,800
小計	25,555,000		2,555,500	22,999,500

台東縣政府　　單位：新臺幣元

	總經費	其他基金或補助款	地方政府自籌款	行政院補助款
108	18,444,000		1,844,000	16,600,000
109	34,783,000		3,478,000	31,305,000
小計	53,227,000		5,322,000	47,905,000

澎湖縣政府　　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
108	25,223,000		3,623,000	21,600,000
109	31,967,000		3,196,700	28,770,300
小計	57,190,000		6,819,700	50,370,300

十、 預定進度

資安區域聯防預定進度：

時程	累計預定進度(%)	累計預定支用費用(元)	關鍵查核點
107/12	34%	16,046,000	1.完成區域聯防情資系統發包作業。 2.完成區域聯防監控系統發包作業。 3.完成擴大監控服務委外發包。
108/12	66%	31,000,000	1.維運區域聯防情資系統。 2.維運區域聯防監控系統。 3.區域情資威脅定期報告。
109/12	100%	46,610,000	1.維運區域聯防監控系統。 2.維運區域聯防情資系統。 3.區域情資威脅定期報告。

十一、 預期效益

1. 強化基層機關資安防護體質，完備國家資安基礎建設

(1)落實資通安全責任等級資安防護要求，強化網站及機關本身資安體質，減少曝露在外的風險。

(2)藉由 GCB 導入可降低成為駭客入侵管道，進而引發資安事件之疑慮。

(3)配合導入 GCB，強化基層機關個人電腦作業系統安全，減少遭駭客利用 Windows XP、Windows Server 2003 伺服器漏洞之風險。

(4)弱點掃瞄管理共同平台各級機關可依需求執行弱點掃描檢測，並可掌握系統已知弱點進行防禦及修補措施。

(5)強化縣市資安縱深防護及基層資安防護：

a.強化政府基層資安防護及區域聯防

- 打造可視化平台(如解密 HTTPS)，透過可視化平台，透視整體網

路流量，當可視性提昇後，資安設備可以看的更多更廣，如此可以及早在惡意程式植入之時或是擴散的時候予以及時的阻絕於第一時間。

- 透視加密網路流量，解決惡意攻擊控制流量加密化之趨勢：越來越多的攻擊趨勢將隱藏在加密的網路流量之中，讓所有資安設備無法透視此網路流量，造成資安的死角，因此透視加密流量，將所有加密流量解密，這樣一來可以讓加密流量不再是資安的盲點。
- 擴大資安設備內網偵測及防範範圍：現在資安設備均防護在外對內的攻擊，以這次 WanaCry 攻擊事件來看，此攻擊手法，跟以往的勒索軟體來比已經從單點進而做橫向擴散至全面的內網之中，因此擴大資安設備的防護範圍不再只有在某一個區塊或是某一個面向的防護，而將整體資安防護擴大到整個網路。
- 虛擬及實體網路可視化提昇：以往資安的佈署均著重於實體網路之中，然而越來越多主機及端點都紛紛導入至虛擬化，因此虛擬化的監控也越來越重要，然而虛擬化的監控不像實體網路一樣，很多網路交換均透過內部虛擬的交換器進行網路資料的交換，因此虛擬化網路也是刻不容緩的一個防禦目標，全面提昇虛擬化與實體網路的監控，達到整體網路無死角的防禦新架構。

b.強化內網防禦機制：

- 強化已知及未知之攻擊：現在的攻擊趨勢已經無法靠特徵碼的防護方式為主要的防禦佈署架構，而需要端點防護與核心資安設備雙管齊下的整體式防護，讓已知的攻擊無法進入，讓零時差攻擊能夠予以防護。

c.都會級別-政府機關的區域聯合防禦機制

- 資安攻擊資訊共享及不同系統間的關聯性整合，以達到區域資安聯防。

2 建立資安區域聯防監控，建立鄰近縣市資安聯防機制

(1)各級機關監控服務

- A 及 B 級機關除維持既有資安監控收容，C+及 C 級機關進行外部出口端的情資聯防設備之資安監控，以達成區域情資蒐集，降低

區域資安死角。

(2)區域聯防監控系統

- 區域聯防中心負責蒐集各機關資安監控事件單，統計底下各機關攻擊分析事件，依技服資安聯防監控月報格式，進行資安監控區域資料統計。
- 定期依資安監控區域資料統計定期產出資安趨勢，每季召開區域資安趨勢分析會議，並提供各級資安威脅情資分析服務諮詢，掌握區域資安事件趨勢並達到所見即所得之資安聯防效益。

(3)部署情資聯防設備

- 部署機關外部出口的情資聯防設備(如:UTM)，以自動化流程派送防護規則(如:新惡意中繼站)，達到區域聯防阻擋效果

(4)區域聯防情資系統

- 可即時掌握國內外情資整合查詢功能並能整合國內外弱點攻擊手法、弱點資料庫，國內外高風險惡意阻擋清單(IP/DN/FQDN)、可自動化產出資安弱點分析情報與資安新聞焦點，區域內最新攻擊熱點呈現，掌握攻擊脈動。

(5)聯防設備防護規則派送

可即時防護並遠端派送防禦阻擋規則(如:技服新公告之惡意中繼站)。

3.建立資安事件快速應變小組及處理流程:協防所屬鄰近縣市並提供資安諮詢或技術支援。

4.資訊安全教育訓練:藉由實務操作演練、持續教育訓練，厚植 機關人才資源，逐步建立資安自主作業能量。

5.結合地區大學能量合作:藉由資通安全學程訓練之學生參與前瞻計畫區域聯防規劃，體驗資通安全實務，並能有機會實務體驗與了解前瞻計畫資安聯防推展之目的與效益。

十二、 相關聯絡資料

(含單位、聯絡人姓名、電話、E-mail 等)

單位	聯絡人姓名	電話	E-mail
高雄市政府	盧漢信	07-7995678 #1318	jason41@kcg.gov.tw
屏東縣政府	李晏彰	08-7320415 #6339	a001487@oa.pthg.gov.tw
台東縣政府	盧貴聰	089-340785	j3020@taitung.gov.tw
澎湖縣政府	陳蕙芝	06-9274400 #293	amychen@mail.penghu.gov.tw