政府科技發展中程個案計畫書

審議編號：108-3601-06-20-03

行政院資通安全處
「強化國家資安基礎建設計畫」

計畫全程：107 年 1 月至 109 年 12 月

107 年 8 月

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">108-3601-06-20-03</td></tr>
<tr><td>計畫名稱</td><td colspan="5">強化國家資安基礎建設計畫</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">經濟部、通傳會</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127,000千元
■109年度前瞻基礎建設額度120,000千元</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">107 年 01 月 01 日 至 109 年 12 月 31 日</td></tr>
<tr><td>中英文關鍵詞</td><td colspan="5">資訊安全、關鍵資訊基礎設施保護、跨域資安聯防、關鍵資安技術
Cyber Security、Critical Information Infrastructure Protection (CIIP)、Cross Domain Cyber Security、Critical Security Technology</td></tr>
<tr><td rowspan="10">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>107</td><td colspan="2">199,000</td><td colspan="2">12.3</td></tr>
<tr><td>108</td><td colspan="2">127,000</td><td colspan="2">8.5</td></tr>
<tr><td>109</td><td colspan="2">120,000</td><td colspan="2">8.3</td></tr>
<tr><td>合計</td><td colspan="2">446,000</td><td colspan="2">29.1</td></tr>
<tr><td rowspan="4">108 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>25,350</td><td>其他資本支出</td><td>101,650</td></tr>
<tr><td>經常門小計</td><td>25,350</td><td>資本門小計</td><td>101,650</td></tr>
</table>

<table>
<tr><td rowspan="8"></td><td></td><td colspan="2">經費小計(千元)</td><td colspan="2">127,000</td></tr>
<tr><td rowspan="6">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>27,500</td><td>其他資本支出</td><td>92,500</td></tr>
<tr><td>經常門小計</td><td>27,500</td><td>資本門小計</td><td>92,500</td></tr>
<tr><td colspan="2">經費小計(千元)</td><td colspan="2">120,000</td></tr>
<tr><td colspan="5"></td></tr>
<tr><td colspan="5"></td></tr>
<tr><td>政策依據</td><td colspan="4">1.FIDP-20170201040000：前瞻基礎建設計畫：1.4 強化國家資安基礎建設
2.NICSP-20170501000000：國家資通安全發展方案(106 年至 109 年)：5.1 建立國家資安情資整合及預警中心
3.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="4">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="4">1.FIDP-20170201040000：前瞻基礎建設計畫：1.4 強化國家資安基礎建設</td></tr>
<tr><td>本計畫在機關施政項目之定位及功能</td><td colspan="4">本計畫在落實第五期國家資通安全發展方案(106 年至 109 年)所訂之「建構國家資安聯防體系」策略，並以水資源及通訊傳播等關鍵基礎設施領域為主，全面打造數位國家所需之資安聯防基礎建設。</td></tr>
<tr><td>計畫重點描述</td><td colspan="4">優先推動水資源及通訊傳播領域之資安防護，並建立重要關鍵資訊基礎設施領域之資安資訊分享及分析中心(ISAC)、資安通報應變中心(CERT)及資安監控中心(SOC)。</td></tr>
<tr><td>最終效益
(end-point)</td><td colspan="4">■ 無修正。
一、建置經濟部及水資源領域之資安資訊分享及分析(E/W-ISAC)平台、資安通報應變 (E/W-CERT) 平台、二線資安監控平台(E/W-SOC)平台。
二、建置通訊傳播領域之新一代資通安全中心(C-SOC)、通報應處平台(C-CERT)、資安訊息分析與分享中心(C-ISAC)。
□ 滾動修正。</td></tr>
<tr><td>主要績效指標
(KPI)</td><td colspan="4">一、完備關鍵資訊基礎設施領域(水資源、通訊傳播)之資安訊息分析及分享中心(ISAC)，
(1) 經濟部：107 年度服務範圍包括：公民營油、氣、電等領域，108 年度將持續擴充水資源領域及經濟事務財團法人，預計服務擴增至 10%，109 年度擴增 30%。
(2) 通傳會：107 年預計完成六大關鍵基礎設施領域業者之納管與通報，包含有：行動通信、固定通信、衛星通信、有線電視、國際海纜及 DNS 網域，後續將針對分析模組進行擴建，並於 108 年完成 80%業者之收容與介接，109 年完成 100%業者介接。
二、完備關鍵資訊基礎設施領域(水資源、通訊傳播)之電腦緊急事故處理小組(CERT)。
三、完備關鍵資訊基礎設施領域(水資源、通訊傳播)之資安監控中心(SOC)，提供通傳事業與水資源領域之資安事件分析及分享與鑑識服務，預計每季提供分析報告一份。</td></tr>
<tr><td>前一年計畫或相關聯之前期計畫名稱</td><td colspan="4">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>

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	-	107 年度完成 E-ISAC，服務範圍包括：公民營油、氣、電等領域，績效指標將在資安旗艦計畫呈現，預計服務 5 家業者	108 年度於本計畫將擴充水資源領域及經濟事務財團法人，預計服務擴增至 10%	109 年度服務擴增至 30%	經濟部關鍵資訊基礎設施領域之 E-ISAC、E-CERT、E-SOC 及 W-ISAC、W-CERT、W-SOC
		-	通傳會規劃於 107 年完成六大關鍵基礎設施領域業者之納管與通報，包含有：行動通信、固定通信、衛星通信、有線電視 SO、國際海纜及 DNS 網域，完成資料蒐集之定義及蒐集方式，後續將針對分析模組進行擴建	108 年完成 80%業者之收容與介接	109 年完成 100%業者介接	通傳會關鍵資訊基礎設施領域之 ISAC、CERT、SOC
		-	1 份	1 份	1 份	提供通傳事業與水資源領域之資安事件分析及分享與鑑識服務，預計每季提供分析報告一份
		-	1 項	1 項	1 項	實測推薦我國資安優質產品(項)
			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)

人力需求及配置說明

一、經濟部

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經濟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。

單位：人/年

計畫名稱	108 年度							109 年度
	總人力	職級						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、建置關鍵基礎設施安全防護計畫(水資源)	0.6	0.3	0.3					0.6
二、經濟部關鍵資訊基礎設施資安資訊分享與分析平台計畫	0.9	0.3	0.3	0.3				0.7

二、通傳會

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通傳會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「國家通訊傳播委員會推動通訊傳播產業創新研究發展補助辦法」等規定，補助財團法人、行政法人、社團法人、學術機構或政府研究機關(構)，辦理數位匯流資通安全分析管理平臺建置與服務。

單位：人/年

計畫名稱	108 年度	109 年度

	總人力	職級						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	
數位匯流資通安全分析管理平臺建置與服務	7	3.5	3	0.5				7

經費需求表(B005)

經費需求說明

推動關鍵基礎設施資安防護，強化水資源領域之關鍵資訊基礎設施資安防護，並建置經濟部關鍵資訊基礎設施領域之資安資訊分享及分析平台(E-ISAC) ，以強化資安聯防。

一、經濟部

單位：千元

計畫名稱	計畫目標	計畫性質	108 年度							109 年度		
			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、建置關鍵基礎設施安全防護計畫(水資源)	建構國家資安聯防體系	其他	40,000						40,000	40,000		40,000
二、經濟部關鍵資訊基礎設施資安資訊分享與分析平台計畫	建構國家資安聯防體系	其他	20,000						20,000	20,000		20,000

經費需求說明

本計畫係推動關鍵基礎設施資安防護，發展防護基本政策與防護基準，並建立通訊傳播網路安全防護中心(CNSPC)及各關鍵基礎設施領域之資訊分析與分享平臺(C-ISAC)、資安通報應變平臺(C-CERT)及資安監控平臺(C-SOC)。

二、通傳會

單位：千元

計畫名稱	計畫目標	計畫性質	108年度							109年度		
			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			
數位匯流資通安全分析管理平臺建置與服務‧	建構通傳業者資安聯防體系	其他	67,000			25,350			41,650	60,000	27,500	32,500

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	107 年度 法定數(千元)	108 年度 申請數(千元)	109 年度 申請數(千元)
經濟部	本院資安處	強化政府基層機關資安防護及區域聯防計畫-經濟部	55,000	60,000	60,000
通傳會	本院資安處	強化政府基層機關資安防護及區域聯防計畫-通傳會	60,000	67,000	60,000
國發會	本院資安處	強化政府基層機關資安防護及區域聯防計畫-國發會	84,000	0	0
各額度經費合計			199,000	127,000	120,000

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

註：500 萬元以上科學儀器請優先考量共用現有設備，並可至「貴重儀器開放共同管理平台」查詢同類儀器；如經查詢現有設備有規格不符需求、開放時段不敷使用、至設備所在位置交通成本偏高等情形，再考量購置之必要性。

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：強化國家資安基礎建設計畫

審議編號：108-3601-06-20-03　　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：本計畫優先推動水資源及通訊傳播領域之資安防護，並建立重要關鍵資訊基礎設施領域之資安資訊分享及分析中心(ISAC)、資安通報應變中心(CERT)及資安監控中心(SOC)。

四、審查意見：

1. 建議盤點各機關軟體存在漏洞及即時更新比率。
2. 請補充說明 ISAC、CERT、SOC 之三層架構完成後之管理及營運，及衡量反應的即時性、聯防效率等 Endpoint。
3. 請補充資安自主產品之定義，並研議增加自主產品使用比率之目標。
4. 請補充說明聯防機制 100%之定義。
5. 建議增加軟體及產品控管人員之 Milestone，逐年強化軟體資安品質、找出軟體之後門、確保軟硬體非來自中國生產、了解國外產品之資安關鍵功能等，以確保資安無虞。
6. 請比較 ISAC、CERT、SOC 之管理運作反應即時性、聯防率。
7. 因政府機關及 CIIP 之軟體採外包方式辦理，請資安處協助訂定我國政府及各 CIIP 軟體委外之規範，以降低資安風險。

五、本處回應：

1. 軟體漏洞目前由技服中心定期發布，各機關作業系統、網頁(微軟)將於每個月定期更新，另防火牆、伺服主機及資安設備更新視軟韌體版本而定，如無法更新則汰換新設備。
2. 各關鍵基礎設施(Critical Infrastructure, CI)領域主管機關，規劃自 106 年

度至 109 年度完成 ISAC、CERT、SOC 建置，並介接至國家層級 N-ISAC、N-CERT、N-SOC，由本院「國家資通安全會報」網際防護體系下設「關鍵資訊基礎設施安全管理組」區分 8 大領域之主責機關維運，本計畫編列特別預算，優先完成能源、通訊、政府骨幹網路等重要關鍵資訊基礎設施之資安防護建置，106 年底各領域主管機關已陸續啟動。107 至 109 年度，將以 Plan-Do-Check-Act(PDCA)循環滾動式修正，達各 CI 領域即時監控應變與完備聯防效益(聯防效率 100%)之目標。

3. 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。預計 109 年度完成政府機關使用國內資安產品比率 50%以上。
4. 有關各 CI 領域之區域聯防機制 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
5. 有關軟硬體是否得境外開發，實務上難有認定標準，目前規劃採由建立檢驗證制度、出具軟體來源及弱點通報等方式，確保軟體安全。本案將參採委員意見，並於 107 年完成資安軟硬體控管機制。
6. 有關 ICS 之三層架構之管理及營運，及衡量反應的即時性、聯防效率，說明如下：
   (1) ISAC：橫向整合跨部會，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：減少機關隱匿資安事件，降低事件誤報與漏報、區域聯防國家整體防護規劃，減少重複投資。

(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。

7. 目前技服中心已訂定「政府資訊作業委外安全參考指引」及「安全軟體設計/測試/發展參考指引」提供政府機關辦理軟體委外或開發之參考指引，未來資安管理法子法亦會訂定相關規範。

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 c.請增人力之類別及進用方式		✓			

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	
	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	職稱：分析師	身份：▓業務單位人員
電話：02-33568061	e-mail：involute@ey.gov.tw	□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	強化國家資安基礎建設計畫		
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	推動關鍵資訊基礎設施資安防護，發展防護基本政策與防護基準，並建立重要關鍵資訊基礎設施領域之資安資訊分享及分析中心(ISAC)、資安通報應變中心(CERT)及資安監控中心(SOC)。	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	本計畫由經濟部與通傳會，於本院性別平等會網站之性別統計專區，統計進用人力之性別統計，查經濟部及所屬共 4,873 人，男性 3,011 人、女性 1,862 人;另通傳會共 458 人，男性 274 人、女性 184 人，其中參與本案之人員符合性別比例 1/3。	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	本計畫將由經濟部與通傳會，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、 建構國家資安聯防體系。。 二、 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。 三、 本計畫將將以鼓勵女性參與，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。	
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)	本計畫將由各機關之主管部門宣導性別平等綱領所揭之重要政策，並鼓勵各部門發展積極策略，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。	

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) 是	評定結果(請勾選) 否	評定原因	備　註
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	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」。

			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。

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	整體計畫已循程序報請審查，其中資安精英人才培育，係由教育部及經濟部研提相關計畫，該計畫將要求優先考慮性別少數人才，力求以不低於 1/3 為原則，以縮小性別差異；另涉及委外招標時，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>10-6 問題與需求評估說明之合宜性</td><td colspan="3">4-2 與本計畫相關之性別統計(如資訊相關科系大學部、研究所及師資研究人員)與性別分析(未來培育及展望)均無。</td></tr>
<tr><td>10-7 性別目標說明之合宜性</td><td colspan="3">性別目標(伍)可再補充，本計畫策略四：孕育優質資安菁英人才。資安人才培育時的性別目標宜明敘。</td></tr>
<tr><td>10-8 性別參與情形或改善方法之合宜性</td><td colspan="3">僅說明「本計畫將於研擬、發展、執行等階段，針對競標廠商就業人口性別進行評估」(陸)，宜明敘依據何標準，如何評估。</td></tr>
<tr><td>10-9 受益對象之合宜性</td><td colspan="3">合宜</td></tr>
<tr><td>10-10 資源與過程說明之合宜性</td><td colspan="3">待補充，例如拔擢在職資安優秀人才，進行資安精英人才培育時，優先考慮性別少數人才，力求以不低於 1/3 為原則，以縮小性別差異。</td></tr>
<tr><td>10-11 效益評估說明之合宜性</td><td colspan="3">待補充，預防或消除性別隔離需有積極作為，設定明確政策目標，而非僅鼓勵增加女性人員。</td></tr>
<tr><td>10-12 綜合性檢視意見</td><td colspan="3">本計畫「策略四：孕育優質資安菁英人才」已明確指出將
∗　鼓勵大專院校開設資安學程，並推動中小學將資安素養議題融入課程教學。
∗　拔擢在職資安優秀人才，進行資安精英人才培育
∗　培育政府機關資訊與資安專職人才。
無論是人才培育或師資邀請，均應配合目前資訊人力的性別統計資料，在執行時的每一環節，設定明確目標，以積極作為縮小性別落差。</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：強化國家資安基礎建設計畫
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	參照國家科學技術發展計畫(106 年-109 年)訂定之(1)研發新興資安技術；(2)發展我國資安科技應用服務，經檢視本計畫由經濟部及通傳會執行之兩項計畫，均係以建置水資源及通傳領域之 ISAC、CERT 與 SOC 為主要工作項目，較少述及新興資安技術之研發應用、相關專業人才之培訓、技術標準與規範之建立等，以及如何推動國內自主技術研發與應用之策略。例如，所建置之各種平台究係採用國外市場之商業軟體或平台，或是部分或全部採購運用本土自主研發之軟體或平台，或採逐步漸進的推動策略與市場主要軟硬體技術及服務提供者共同合作研發或以工業合作技術移轉，本案執行團隊宜有更完整的論述或規劃。	有關委員所提新興資安技術之研發應用、相關專業人才之培訓、技術標準與規範之建立等工作，已有資安旗艦計畫及資安產業發展行動計畫進行推動，本計畫著重經濟部(資訊中心、水利署)及通傳會之建構資安聯防體系」為主。 由於本計畫所需之技術為市場成熟技術，研發需求不高，惟著重使用國產品之成分，將請計畫提報機關加強使用國產品之論述。	p.4 p.48
2	目前國內不管是學術研究界、產業界及政府機關及私人企業等，少有推動 OT 相關的推動經驗、專業人員相對不足，亦未有自主開發相關平台，建議參考主要國家之推動經驗(例如美國國土安全部 NCCIC 及 ICS-CERT)並盤點國內當前的產學研資安技術研發量能，推動本計畫研發及應用新興資安技術及發展我國資安科技應用服務之工作事項。	1.本院今年 3 月通過之資安產業發展行動計畫已規劃建立資安研訓院，培育國內資安人才，並將 OT 人才培育列為優先選項，期望藉此提升我國於 OT 領域專才之質與量。 2.另科技部辦理資安前瞻創新研發計畫之分項計畫亦是提升 OT 人才培育能量，例如：中興大學 TWISC，著重於關鍵資訊基礎設施(CIIP)領域之資安與隱私防護機制研發，培育能源(電廠)領域之 OT 人才。	-

3	本計畫的目標為完備水資源關鍵基礎設施之資安防護。107 年著重在 W-ISAC 及 W-CERT 建置。惟此兩機制仰賴是否將水利署散佈在臺灣各地的水利設施例如水庫及河川監控之營運資料收集與分析，釐清可能的資安事件與等級，這屬於 SOC 的維運，是完備資安防護的根本基礎。沒有完備之 SOC，談不上 ISAC 與 CERT 是否能發揮功效。	水利署為完備水資源關鍵基礎設施之資安防護，需持續擴充 W-ISAC 功能與情資類型，以達資安資訊分享，另建置 W-CERT 平台作為關鍵基礎設施資安事件通報機制之基礎，藉此強化各水庫、堰、壩關鍵基礎設施同仁資安意識。 W-ISAC、W-CERT、與 W-SOC 在資安防護工作實屬環環相扣，需能緊密結合，以期發揮資安防護綜效，水利署經濟部已導入 SOC 監控維運，並規劃自 108 年度起各水資源局、河川局陸續導入 SOC 監控維運，建立一線 SOC 之基礎並結合 W-SOC(二線 SOC)，以建立水利署資安聯防機制，提升資安預警能力。	-
4	本案以建置 E/W-CERT、E/W-ISAC 及 E-W/SOC 軟硬體平台及自動化資訊蒐集交換及自動或人工介接為工作重點，惟尚待加強推動關鍵的 OT 資安專業人才培訓與觀念推廣、風險管理、資安稽核及審驗、演練、事件通報應變及復原、技術標準與規範研訂以及區域或國際合作等相關配套措施。	本院今年 3 月通過之資安產業發展行動計畫已規劃建立資安研訓院，培育國內資安人才，並將 OT 人才培育列為優先選項。 另針對風險管理、資安稽核及審驗、演練、事件通報應變及復原、技術標準與規範研訂等，水利署將於 108 年度完成水資源領域之資安事件通報與演練等規範。	p.57-p.61
5	整個計畫書目前只有大目標，具體執行內容欠缺。建議 108 年度納入：a) 盤點全臺灣水資源建在資安防禦層面需要監控的模組，不應只是包含 107 年度的資訊資產盤點，所有 OT（operations technology）設施與系統的部分應納入; b) 設施監控之必要收集的資料定義、資料收集方式與分析模組；c) 水資源需通報之資安事件的定義，以釐清並確實知道在 ISAC 資安事件通報的具體可能事件以及 CERT 應變措施。	(1)水利署 108 年度的資訊資產盤點，係延續 106 年度及 107 年度的計畫，擴大資訊資產盤點的範圍，並已包括 OT 設施與系統的部分。水利署 106 年度的資訊資產盤點主要範圍為北區水庫單位，107 年度則為中區水庫單位，108 年度則為南區水庫單位。 (2)水利署已建備水情監測、閘門控制等系統，已完成設施監控之必要資料收集與監測，惟因考量 OT 相關設施之特性(OT 系統需確保可用性)，與專屬網路通訊協定，OT 相關系統暫未導入 SOC 資安監控，目前以閘道或網路邊界建置相關資安防護設備，例如：防火牆系統。 (3)水利署將配合於 108 年度計畫納入「水資源需通報之資安事件的定義」規劃。	p.57-p.61

6	計畫書所列之實體安全監控應納入本計畫。但是「高效能源管理」、「建置虛擬化基礎平台」、「行動裝置管理」似乎與本計畫目標不符，建議檢討或移除。	水利署將依委員建議、進行計畫書內容調整，移除「高效能源管理」、「建置虛擬化基礎平台」、「行動裝置管理」。	p.55
7	分項計畫二有關 ISAC 平台的擴充，目前規劃的項目應強化資安情資的深度、必要性與重要性的挑選。	謝謝委員的建議。本計畫除 ISAC 平台功能性的擴充外，將進一步規劃強化資安情資的深度。	-
8	本計畫的執行內容與計畫目標不符。建置通訊 N─SOC、N─ISAC、N─CERT，是要完備傳播通訊關鍵基礎設施遭受威脅與攻擊時的偵測、通報與危機處理。此目標的達成，在 107 年度完成資料交換的標準格式化，只是一小步。如何將臺灣各業者的通訊網路設施的監控資料收集與分析，釐清哪些是關注的資安事件與等級，這是屬於 SOC 的維運，是完備資安防護的根本基礎。沒有完備的 SOC，談不上 ISAC 與 CERT 是否能發揮功效。	以目前關鍵基礎設施(CI)之資安防護需求而言，急需建立各 CI 接受外部情資之管道，以提早防範資安事件與即早進行應處，爰調整聯防建置順序，以完備 ISAC 為優先，至於 SOC 部分，因部分關鍵基礎設施主管機關過去已建置 SOC，惟未完備，故以計劃餘裕經費逐步建立。 本計畫所關注的對象為通傳業者關鍵資訊基礎 CII 設施，其遭受資安威脅影響涉及網際網路用戶服務之權益，監控來自外部攻擊之資安事件。業者通報至 C-SOC，由 C-SOC 擔任二線監控與即時分析，針對低影響等級之攻擊事件，透過持續性的觀察監控、分析攻擊手法，將相關情報資訊透過 C-ISAC 管道分享給其他業者，達到初級預警效益。針對中高影響等級之攻擊事件或已發生對用戶服務造成影響之攻擊事件，啟動 CERT 機制。 此外針對事件處置過程，透過去識別化與 C-ISAC 分享機制，分享其他業者，降低災害擴大情形。藉由業者通報所遭受外部攻擊之原始數據（不具營業秘密），進一步釐清及反映通傳領域的資安態勢。	-

9	整個計畫書的執行內容沒有看到專注於「關鍵」的議題，建議重擬。本案目前的執行內容，只是花錢建了三個框架，缺乏實質的研發內涵。	本計畫透過 107 年系統框架之建置，將於 108 年逐步研究網際網路服務業者關鍵資訊基礎設施弱點模組之誘捕系統研發，結合 107 年系統框架之建置，擴大誘捕威脅樣本，協助通傳領域發掘威脅活動，分享相關情資至通傳事業。	p.82-p.83
10	本計畫的執行太過被動、不夠積極與負責：「輔導通傳事業 SOC 與 C-SOC 建立自動化方式資訊傳遞 」、「協助無自建 SOC 之通傳事業資安防護設備日誌分析資安事件或輔導業者建置自主監控分析能力」，應更積極明確地告知，108 年度、109 年度，會有多少的業者，多少比例的通訊關鍵基礎設施，哪些重要事件會被通報等等會納入整個通訊資安防禦偵測、通報與應變體系。	本計畫預計 108 年度輔導 17 家無自建 SOC 或資安監控、分析系統之通傳事業，透過由 C-SOC 蒐集 IntrusionPreventionSystem(IPS) 、Firewall(FW)、AntiVirus(AV)等來自外部攻擊日誌資訊進行監控，進一步協助分析取得該業者之資安事件通報予該通傳業者完成資安事件通報與分享機制。	p.82-p.83
11	建議 108 年度納入： a) 盤點全臺灣通訊設施在資安防禦層面需要監控的設備、服務等，所有 OT（operations technology）設施與系統的部分應納入; b) 設施監控之必要收集的資料定義、資料收集方式與分析模組；c) 需通報之資安事件的定義，以釐清並確實知道在 ISAC 資安事件通報的具體可能事件以及 CERT 應變措施。	通傳會已於公務預算編列「數位匯流/IoT 資安威脅防禦機制暨資安實驗室建置與服務計畫」，該計畫包含網路運作管理平臺建置(NOMC)。通傳會於 107 年完成六大關鍵基礎設施 CI 之納管與通報，包含有：行動通信、固定通信、衛星通信、有線電視 SO、國際海纜及 DNS 網域，完成資料蒐集之定義及蒐集之方式，後續將針對分析模組進行擴建，於 108 年完成 80%業者之收容與介接，並預計於 109 年滿足 100%業者介接。本計畫則以 CIIP 為主要防護標的。 通傳會除了過 NOMC 了解六大關鍵基礎設施之狀態外，並結合網際網路服務提供之業者之資安事件監控，具體瞭解資安事件之關連性，並透過 C-ISAC 管道分享給其他業者，達到初級預警效益。針對中高影響等級之攻擊事件或已發生對用戶服務造成影響之情事，除了透過 C-ISAC 進行分享外，也立即啟動 CERT 應變措施。	p.79-p.80

12	請釐清「蒐集 IASP 佈點主機及國外移案之垃圾郵件資訊，產出統計報表，並通報至 C-CERT 及 C-ISAC 進行應處及分享 」與政策以及本計畫的關連性與必要性。	有關蒐集 IASP 佈點主機及國外移案之垃圾郵件資訊,產出統計報表,並通報至 C-CERT 及 C-ISAC 進行應處及分享機制，本計畫於 108 年度建置主動分析系統，將垃圾郵件中除了廣告類型郵件外，亦隱藏了許多惡意郵件或釣魚郵件所衍生之資安事件威脅，透過分析垃圾郵件樣本，以及駭客探測信規則，建立相關手法及樣本知識庫，並透過 C-ISAC 管道進行分享,提供通傳事業以建立防禦偵測機制。	-
13	水利署： 建議增加 KPI: a) 以 108 年度將會納入資安防禦體系的全臺灣水資源設施與系統的個數與比例; b) 設施監控之必要收集的資料定義、資料收集方式與分析模組；c) 水資源需通報之資安事件的定義、數量、重要等級；d) ISAC 資安事件通報的涵蓋範圍、數量與比例；e) 具體各重要事件 CERT 的應變措施之數量與比例。	經濟部水利署配合調整計畫內容，將於 108 年度納入資安防禦體系之全臺灣水資源設施單位數量，惟考量 108 年度尚再進行資訊資產盤點作業，因此暫未納入系統的個數。 經濟部水利署已建備水情監測、閘門控制等系統，已完成設施監控之必要資料收集與監測,惟因考量 OT 相關設施之特性與專屬網路通訊協定，為確保 OT 系統可用性，避免資安監控作業影響 OT 系統正常運行，因此 OT 相關系統未導入 SOC 資安監控，而暫未納入目前計畫 KPI。 有關經濟部水利署配合調整計畫內容，需進一步研擬資安事件之定義與重要等級，惟考量未能預期資安事件數量,而未納入目前計畫 KPI。 有關「ISAC 資安事件通報的涵蓋範圍」,經濟部水利署將配合調整計畫內容，另有關「ISAC 資安事件通報的數量與比例」,惟考量未能預期資安事件數量與比例，而未納入本計畫 KPI。	p.68- p.71
14	請確認且訂正- page: 1-3: 正確的主要績效指標（KPI）應該是: 三 資訊服務：提供通傳事業資安事件分析及分享與鑑識服務，預計每季提供分析報告一份(page: 1-6)。而非，三、完備關鍵資訊基礎設施領域(水資源、通訊傳播)之資安監控中心(SOC)。	本計畫將遵照委員意見調整，增加績效指標（KPI）：提供通傳事業資安事件分析及分享與鑑識服務，預計每季提供分析報告一份。	p.3 p.4 p.48

15	請於計畫書中補述詳列 107 及 108 年分年績效指標及全程績效指標，並與最終效益(End Point) 的相依性，以利檢視各里程碑的成果。	本計畫將遵照委員意見調整，詳列 107 及 108 年分年績效指標及全程績效指標，並與最終效益(End Point) 的相依性，以利檢視各里程碑的成果。	p.4 p.47
16	請確認本計畫 page:14；參、執行策略及方法項目之年度 106 107 108 109 及績效指標與量化指標(%)之內容的正確性? 另發現 108 年度執行之計畫量化指標內容不一致性。	本計畫將遵照委員意見調整，確認 106、107、108、109 之執行策略及方法項目，另重新檢視績效指標與量化指標(%)之內容的正確性。	p.4 p.48 p.68-p.71 p.82-p.83
17	建議增加 KPI: a) 以 108 年度將會納入資安防禦體系的全臺灣各業者的通訊網路設施的與系統的個數與比例； b) 設施監控之必要收集的資料定義、資料收集方式與分析模組；c) 需通報之資安事件的定義、數量、重要等級；d) ISAC 資安事件通報的涵蓋範圍、數量與比例；e) 具體各重要事件 CERT 的應變措施之數量與比例。	通傳會將參採委員建議，將所述意見項目納入 KPI，增加 a) 以 108 年度將會納入資安防禦體系的全臺灣各業者的通訊網路設施的與系統的個數與比例； b) 設施監控之必要收集的資料定義、資料收集方式與分析模組；c) 需通報之資安事件的定義、數量、重要等級；d) ISAC 資安事件通報的涵蓋範圍、數量與比例；e) 具體各重要事件 CERT 的應變措施之數量與比例。	p.82-p.83
18	請補充 KPI- 108 年度、109 年度，各會有多少業者，多少比例的通訊關鍵基礎設施，哪些重要事件會被通報等納入整個通訊資安防禦偵測、通報與應變體系中。	通傳會規劃於 107 年度完成六大關鍵基礎設施之納管與通報，包含有：行動通信、固定通信、衛星通信、有線電視 SO、國際海纜及 DNS 網域，同時結合網際網路服務提供業者之資安事件監控，具體瞭解資安事件之關連性，另 108 年完成 80%業者之收容與介接，並於 109 年滿足 100%業者介接，針對網際網路服務之業者，規劃於 108 年完成涵蓋我國網際網路使用用戶數達 80%，至 109 年逐步擴大涵蓋我國網際網路服務業者加入資安通報應變體系中。	-

19	請修正最終效益(end-point) (質化+量化)與主要績效指標(一定要量化)，以利評估最後效益(end-point)是否達成。	量化績效修正： (1)完成 C-SOC 平臺蒐集 17 家無自建 SOC 通傳事業之資安防護設備日誌，協助分析資安事件。 (2)完成 C-CERT 平臺與 24 家通傳事業(含新增 12 家)之資安事件通報與回報雙向介接 1 式。 (3)完成 C-ISAC 平臺與 24 家通傳事業(含新增 12 家)之資安訊息分享雙向介接 1 式。 (4)完成 C-ISAC 平臺分享資安情資至 IASP 業者，每年至少 15,000 筆。 (5)完成 C-ISAC 平臺分享資安情資至 N-ISAC，每年至少 6,000 筆。 (6)完成 C-ISAC 平臺移案垃圾郵件至 IASP 業者，每年至少 30,000 封。 (7)完成 C-ISAC 平臺與合作國交換垃圾郵件，每年至少 80,000 封。 (8) 完成 C-ISAC 平臺經由 TWCERT/CC 與非合作國交換垃圾郵件，每年至少 300,000 封。	p.82-p.83
20	本案將辦理弱點掃描、攻防演練及資安情資分享檢討會議等，作為人才培育，惟部分關鍵績效指標，似無法具體呈現該項目之實質效益，建請評估其妥適性。	人才培訓績效調整為參加國際 AntiSPAM、HoneyProject 技術研討會，掌握防制 SPAM 及佈點主機誘捕最新技術　取得國際資安證照：GIAC 系列、ISMSLeadAuditor、CISSP、Security+、ECSA、CEH、CISA 或 CHFI 證照等資安證照至少 4 張。註：為具體呈現整體績效，本項目將參採委員意見挪至公務預算執行。	-
21	本計畫可加強與經濟部、教育部及科技部執行之資安人才培訓及資安產業發展相關計畫連結。	本計畫將參採委員意見加強與其他計畫資安人才培育及資安產業發展計畫之連結，其績效指標將於資安旗艦計畫呈現。	-

22	本計畫可加強與國發會規劃執行之物聯網資安分享計畫連結。	本計畫將參採委員意見，由行政院資安處進行跨部會協調，將與物連網資安分享計畫之連結合作考。	-
23	本計畫可加強與科技部及經濟部規劃推動與大數據及人工智慧有關的計畫連結，俾能將人工智慧及大數據運用於資安事件分析。	本計畫現行情資分享等機制已多考量使用人工智慧及大數據技術進行分析，另本院人工智慧行動計畫中亦有將資安議題納為其研究議題之一，本計畫後續將密切推動前述技術於資安領域的應用。	-
24	本計畫部分工作項目與「資安旗艦計畫」建置各領域關鍵基礎設施資安資訊分享及應變中心內容雷同，有檢討整併空間。	本計畫著重建置水資源、通傳等領域之關鍵基礎設施聯防機制，其餘領域(例如：電、油、瓦斯)由資安旗艦計畫執行。	-
25	部分所需建置設備的目的、規格、數量缺乏用途說明，從執行內容看不出購買設備之必要性。	本計畫將重新審視計畫採購設備之內容說明是否完備且具體,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。	-
26	本計畫係依據總統「資安即國安」戰略以及行政院第五期國家資通安全發展方案揭櫫之願景、目標及策略，據以研擬水資源及通訊傳播領域之關鍵基礎設施建設計畫，就計畫之必要性、需求性及迫切性，均有必要持續執行。	謝謝委員支持，本計畫將遵照委員意見，依據總統「資安即國安」戰略以及本院第五期國家資通安全發展方案揭櫫之願景、目標及策略，執行各項重要工作。	-
27	本計畫主要核心為水資源及通訊傳播領域之關鍵基礎設施資安基礎建設，並以 iSAC、SOC 及 CERT 等相關資安防護機制之建立為重點工作。惟國內產學研及事業機構對於關鍵基礎設施之 OT 資安專業人才及防護管理實作經驗欠缺。計畫推動初期階段建議參考主要國家之推動經驗(如平台建置、事件分級、	目前除本計畫外，資安旗艦計畫及資安產業發展行動計畫，皆規劃透過資安人才培育、關鍵基礎設施場域提供等具體措施，以逐步落實資安防護工作並提升資安產業自主能量。後續本處亦將落實、精進管考作業，俾協同執行部會達成計畫目標。	-

	風險分析、稽核及審驗等)，逐步累積經驗及培訓人才，期能進一步提升關鍵基礎設施之資安防護及管理量能。		
28	主要績效指標計有三項，為完備關鍵資訊基礎設施領域(水資源、通訊傳播)之 ISAC、CERT 及 SOC, 三項項績效指標均為過程型及產出型之指標，無法衡量本計畫之實際績效，建議經濟部及通傳會研訂「結果型」(outcome)績效指標作為主要績效指標。例如，各關鍵基礎設施提供者對於資安事件之通報應變效率提升情形(例如資安事件平均處理時間、事件發生到完成通報的時間等)、SOC 關聯分析之準確度、對於資安事件由關鍵基礎設施提供者由下而上主動通報與由上而下通報之比例、資安事件減少情形等。	有關委員所提研訂「結果型」(outcome)績效指標作為主要績效指標，經濟部調整績效指標如下： 經濟部： 107 年度完成 E-ISAC，服務範圍包括：公民營油、氣、電等領域，績效指標將在資安旗艦計畫呈現，預計服務 5 家業者，108 年度於本計畫將擴充水資源領域及經濟事務財團法人，預計服務擴增至 10%，109 年度完成 30%。 通傳會： 通傳會規劃於 107 年完成六大關鍵基礎設施領域業者之納管與通報，包含有：行動通信、固定通信、衛星通信、有線電視 SO、國際海纜及 DNS 網域，完成資料蒐集之定義及蒐集方式，後續將針對分析模組進行擴建，於 108 年完成 80%業者之收容與介接，並預計於 109 年完成 100%業者介接。	p.4 p.48
29	為了方便國際接軌，建議行政院資安處參考主要國家的實施經驗，重新檢討目前施行的資安事件分級分類的妥適性，以利今後進行國際合作或區域聯防。(例如，建立類似全世界通行的颱風或地震等級)	有關資安事件分級分類，我國資安事件影響等級分為 4 級，由重至輕分別為「4 級」、「3 級」、「2 級」及「1 級」，各國配合當地政府通報規範與資安事件處理程序進行分級，查各國分級方式皆有所差異，針對委員所提建立類似全世界通行的颱風或地震等級，目前係採用國際標準情資交換格式，例如：STIX(StructuredThreatInformationeXpression)與各國交換情資，此格式分為 9 大模組:資安威脅觀察資料、資安威脅模式、資安威脅事件、資安威脅手法、資安威脅活動、資安威脅者、資安威脅目標、資安威脅防護措施及資安威脅報告等，另資安類型分為資安訊息情資(ANA)、	-

		資安預警情資(EWA)、網頁攻擊情資(DEF)、入侵攻擊情資(INT)及回饋情資(FBI)。	
30	有關國家通訊傳播委員會之執行項目宜再審慎調整，以利政策目標之達成。	謝謝委員支持，本計畫將遵照委員意見，將國家通訊傳播委員會之執行項目宜再審慎調整，以利政策目標之達成。	p.79
31	應妥善運用國內資安社群以及從HITCON成長衍生之創新新創公司，俾利於資安建設過程中，同步茁壯我國資安產業。	本計畫將參採委員意見加強與資安產業發展計畫之連結。	-
32	本案係依據行政院第五期國家資通安全發展方案揭櫫之願景、目標及策略，據以研擬水資源及通訊傳播領域之關鍵基礎設施建設計畫，就「國家安全」的角度而言，本案推動有其必要性及迫切性。	謝謝委員支持，本計畫將遵照委員意見，依據總統「資安即國安」戰略以及本院第五期國家資通安全發展方案揭櫫之願景、目標及策略，執行各項重要工作。	-
33	本案執行單位規劃建立資安研訓院，培育國內資安專業人才。本案主要核心目標為水資源及通訊傳播領域關鍵基礎設施之資安基礎建設，並以ISAC、SOC及CERT等相關資安防護機制之建立為重點工作，建議於資安研訓院中加強培育本案所需之資安專業人才，以完善我國關鍵基礎設施之資安防護。	目前除本計畫外，資安旗艦計畫及資安產業發展行動計畫，皆規劃透過資安人才培育、關鍵基礎設施場域提供等具體措施，以逐步落實資安防護工作。	-
34	本案已規劃主要績效指標，惟此指標皆為產出型之指標，無法衡量實際執行成效，建議研訂「結果型」績效指標作為主要績效指標，例如，各關鍵基礎設施提供者對於資安事件之通報應變效率提升情形(例如資安事件平均處理時間、事件發生到完成通報的時間等)、SOC關聯分析之準確度、對於資安事件由關鍵基礎設施提供者由下	有關委員所提研訂「結果型」(outcome)績效指標作為主要績效指標，經濟部調整績效指標如下： 經濟部： 107年度完成E-ISAC，服務範圍包括：公民營油、氣、電等領域，績效指標將在資安旗艦計畫呈現，預計服務5家業者，108年度於本計畫將擴充水資源領域及經濟事務財團法人，預計服務擴增至10%，109	p.4 p.48

	而上主動通報與由上而下通報之比例、資安事件減少情形等。	年度完成 30%。 通傳會： 通傳會規劃於 107 年完成六大關鍵基礎設施領域業者之納管與通報，包含有：行動通信、固定通信、衛星通信、有線電視 SO、國際海纜及 DNS 網域，完成資料蒐集之定義及蒐集方式，後續將針對分析模組進行擴建，於 108 年完成 80%業者之收容與介接，並預計於 109 年完成 100%業者介接。	
35	除本案所屬領域關鍵基礎設施之推動外，建議行政院資安處亦應進行各領域關鍵基礎設施之相互關聯分析，建立跨領域之通報應變、資訊分享、人才培訓及聯防協作等整體運作機制，俾能善用有限的資源發揮最大的計畫實施效益。	有關各關鍵基礎設施領域之情資關聯分析、跨領域的通報應變、人才培育及聯防協作等整體運作機制，簡要說明如下： 建構國家資安聯防體係：本計畫與資安旗艦計畫，分別完成 8 大關鍵基礎設施領域之 ISAC、CERT 及 SOC，達到跨領域之情資分享、緊急應變及資安監控，以強化縱向通報及橫向通知機制，另掌握國家整體資安風險，即時分析資安事件樣態及駭侵手法，並部署主動式防禦機制，以建立跨域資安聯防機制。 有關資安人才培育，包括在學、在職、政府機關(構)及在營體系之資安人才培育，本處係透過資安旗艦計畫推動主責部會建立領域課程地圖。在教育體系部分，教育部前已著手規劃課程地圖，後續將持續追蹤，由上而下有效推動資安人才培育工作。	-

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	本案係水資源及通訊傳播領域之資安關鍵基礎設施建設計畫，就「國家安全」的角度而言，本案推動有其迫切性。執行單位對資安關鍵基礎設施環境建設已依原規劃執行，並建立各自專案管理機制。本案執行團隊應構思更多元應用服務，如電力、瓦斯等，並落實服務管理平台與終端模組之軟硬體資安檢測，積極導入實際應用場域進行驗測，以提升本案社會實質效益。	1.有關建議納入多元應用服務，如能源領域(電力、油、瓦斯)部分，查經濟部目前已於另一資安旗艦計畫處理，至於本計畫辦理之經濟部水資源領域區域聯防作業，應用機關除水利署署本部外，另含北、中、南三個水資源局以及轄下 15 個水庫。 2.有關服務管理平台與終端模組之軟硬體資安檢測，本計畫將要求計畫主辦機關應遵循資安管理法子法「資通安全責任等級分級辦法」規定，執行「資安健診」、「滲透測試診」、「弱點掃描」等資安檢測，另本院國家資通安全會報採取每年定期辦理資安稽核，確保各政府機關建置周全(robustness)的資安防護，並舉辦攻防演練確認其資安防護是否堅實(resilience)。 3.有關實際應用場域驗測，本計畫將配合資安產業發展計畫，要求計畫執行機關開放資安技術領域可行之試煉場域，帶動我國資安產業發展與創新應用。	-
2	本案宜依國際資安等級訂定國家水資源及通訊傳播領域關鍵基礎設施之資安運作規範，並具體落實與用戶案例驗測。此外，針對規範之可信度、標準規範鏈結程度等，宜具體分析，並持續推動成為國家標準。	1.有關水資源關鍵基礎設施資安運作規範，本計畫規劃於 108 年完成水資源領域之資安防護政策與基準，作為各水庫單位維運水資源關鍵基礎設施之資安防護指引。 2.另通傳會規劃於 107 年度完成「電信關鍵資訊基礎設施資訊系統分級與資安防護基準草案」，針對第一類電信事業（行動通信、衛星固定通信、綜合網路、電路出租及國際海纜）及第二類電信事業(達 10 萬用戶以上者)試行，並完成關鍵資訊基礎設施盤點與分級，以驗證草案可行性，其績效指標將於資安旗艦計畫呈現。 3.有關推動國家資安驗測標準，通傳會規劃於 107 年度，完成國際組織技術規範指引研析，針對通傳終端設備及無線射頻器材等產品，例如無線 Wi-	-

		Fi AP、無線 IP CAM、無人機、電腦無線輸入裝置、無線智慧電表、無線 Wi-Fi 路由器等終端設備，進行資安威脅之研析及資安檢測，並研訂資安檢測技術規範，輔導國內廠商導入及研發符合資安標準之產品，提高國際市場競爭力，其績效指標將於資安旗艦計畫呈現。	
3	本案係水資源及通訊傳播領域之資安關鍵基礎設施建設計畫，本案執行單位對資安關鍵基礎設施之環境建設已依原規劃執行，並建立各自專案管控機制。此外，本案遵循資安管理法之子法「資通安全責任等級分級辦法」規定，執行「資安健診」、「滲透測試診」、「弱點掃描」等資安檢測，另行政院國家資通安全會報將於每年定期辦理資安稽核，確保各政府機關建置周全與堅實的資安防護。	謝謝委員支持，本計畫將遵照委員意見，依據資安管理法之子法「資通安全責任等級分級辦法」規定，執行「資安健診」、「滲透測試診」、「弱點掃描」等資安檢測，另配合本院國家資通安全會報於每年定期辦理之資安稽核，確保各政府機關建置周全與堅實的資安防護。	-

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	本案主要係強化國家資安設備及相關技術，在分項計畫「數位匯流資通安全分析管理平臺建置與服務計畫」將「孕育優質資安菁英人才」列入策略項目，因受「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，及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.21
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」： 請補充參與本案之人員及近年來進用人力之性別統計，如有性別落差較大之情形，請分析落差原因。	本計畫將遵照委員意見，由經濟部與通傳會，於本院性別平等會網站之性別統計專區，統計進用人力之性別統計，查經濟部及所屬共 4,873 人，男性 3,011 人、女性 1,862 人;另通傳會共 458 人，男性 274 人、女性 184 人，其中參與本案之人員符合性別比例 1/3。	p.22

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，由經濟部與通傳會，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.22
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，縮小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.22
5	性別影響評估檢視表第陸項、性別參與情型或改善方法： 建議補充在人才培育及推廣方面，如何鼓勵女性參與之具體做法。	本計畫將遵照委員意見，補充人才培育及推廣，詳述如下： 本計畫將由各機關之主管部門宣導性別平等綱領所揭示之重要政策，並鼓勵各部門發展積極策略，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。	p.22
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.22- p.23

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

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，針對「建構國家資安聯防體系」之強化關鍵資訊基礎設施資安防護措施，舉凡金融、交通、醫療、能源、科學園區、水資源及通訊傳播等重要關鍵基礎設施，本計畫優先完成能源、通訊傳播領域之資安防護建置。

二、擬解決問題之釐清

隨著大數據、物聯網、移動裝置及雲端服務等新興資通訊科技應用普及，網路與實體世界已逐漸融合，新興資通訊科技固然對人類帶來生活的便利，然而伴隨而來的卻是衍生的資安風險，對於民眾生活、經濟活動及國家安全的影響將與日俱增。

近年來，關鍵基礎設施的保護議題，已逐漸成為各國所重視議題，主因在於關鍵基礎設施之防護完備與否，攸關國家安全、政府運作、人民生活、經濟發展與永續生活，依據行政院 103 年 12 月 23 日頒布之「國家關鍵基礎設施防護指導綱要」，我國關鍵基礎設施（CI）分類，詳述如下：

(一) 主部門：分為能源、水資源、通訊傳播、交通、銀行與金融、 緊急救援與醫院、中央與地方政府機關、高科技園區 等八類。

(二) 次部門： 依主部門重要元件之屬性再區分次部門，例如能源主 部門下再區分電力、石油、天然氣、化學與核能材料等次部門。

(三) 重要元件設施： 係指維持設施營運所必須之重要設備、運作系統、通

訊系統、維安系統，以及重要資訊系統或控制、調度 系統等。

前述各類關鍵基礎設施因應資通訊科技發展與潮流，多已應用或導入資通訊系統，用以控制關鍵基礎設施設備之日常運作，而此揭資通訊系統一旦遭受有心人士之惡意攻擊，將嚴重影響關鍵基礎設施之持續運作，爰此，「資安即國安」已為政府宣示之重要政策，為達前述政策目標，本計畫將著重關鍵資訊基礎設施之水資源及通訊傳播領域資安防護，另金融、交通、醫療、能源、科學園區則由資安旗艦計畫推動各執行項目，旨為全面打造數位國家所需之資安基礎建設，做為我國發展數位國家之後盾。

三、目前環境需求分析與未來環境預測說明

本計畫從國家整體防禦面、技術面及產業面，全面打造數位國家所需之資安基礎建設，做為我國發展數位國家之後盾。其經費來源，原自科發基金管理會計畫補助款，但因該經費性質多屬經常門性質，惟資安之建設有部分係屬設備採購，故編列特別預算優先由經濟部、通傳會共同執行。

四、本計畫可發揮之加值或槓桿效果

隨著資通訊科技蓬勃發展，使得資安風險隨之提高，諸如人為疏失、操作不當、駭客攻擊與公務機密外洩等問題，皆已成為攸關社會安定、甚或國家安全之重要議題。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，旨為強化我國關鍵基礎建設領域之資安通報應變及資訊共享機制，進而推廣資安教育訓練及推動資訊安全管理系統驗證等作為，俾能有效提供基礎建設所需之最佳安全保障。另本計畫亦配合資安產業發展計畫，協助資安技術領域之試煉場域，帶動我國資安產業發展與創新應用。

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，透過政府投資提高資安自主比率，並建立跨域合作機制，促成資安整體解決方案，以建立良好口碑，打造臺灣資安優質品牌，另提高科研計畫投入可產品化及前瞻技術研發之比例，結合資通安全研究與教育中心(TWISC)，以理論探討、實務研究及推廣教育等發展主軸，發展相關資安技術與產品，使理論與實務應用相結合。

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

本計畫優先完成能源、通訊傳播領域之資安防護建置，達成目標如下：

(一) 強化水資源關鍵資訊基礎設施之資安防護，防範水資源領域免於遭

受駭客入侵攻擊。

(二) 建構通傳業者之資通訊安全防護機制，強化我國數位匯流及網路資通訊安全，打造數位國家・創新經濟發展方案之「數位創新基礎環境」。

二、執行策略及方法

(一) 經濟部：

推動關鍵基礎設施資安防護，強化水資源領域之關鍵資訊基礎設施資安防護，並建置資安資訊分享及分析(E/W-ISAC)平台、資安通報應變中心(E/W-CERT) 平台、二線資安監控中心(E/W-SOC)平台，以降低資安風險對關鍵基礎設施運作之影響。

(二) 通傳會：

強化通傳事業關鍵基礎設施之資安防護能力，同時建構通訊網路之資通安全分析與管理平臺，包含建立通訊傳播領域之資安監控平臺 (C-SOC)，彙集多元資安情資來源，制定通訊傳播事業之資安通報應變機制(C-CERT)，並提供資安事件分析、資安趨勢、資安關聯之資訊分析與分享(C-ISAC)，以降低資安事件所衍生之風險，保障國內資通安全與人民權益。

三、目標實現時間規劃

(一) 建置關鍵基礎設施安全防護計畫(經濟部)

108 年度預定進度

時程	累計預定進度(%)	關鍵查核點
108 年 3 月	10%	完成 108 年度專案管理計畫書
108 年 7 月	50%	完成第二期報告

108 年 10 月	85%	完成第三期報告
108 年 12 月	100%	完成 108 年度期末報告

109 年度預定進度

時程	累計預定進度(%)	關鍵查核點
109 年 3 月	10%	完成 109 年度專案管理計畫書
109 年 7 月	50%	完成第二期報告
109 年 10 月	85%	完成第三期報告
109 年 12 月	100%	完成 108 年度期末報告

(二) 建置關鍵基礎設施安全防護計畫(通傳會)

108 年度預定進度

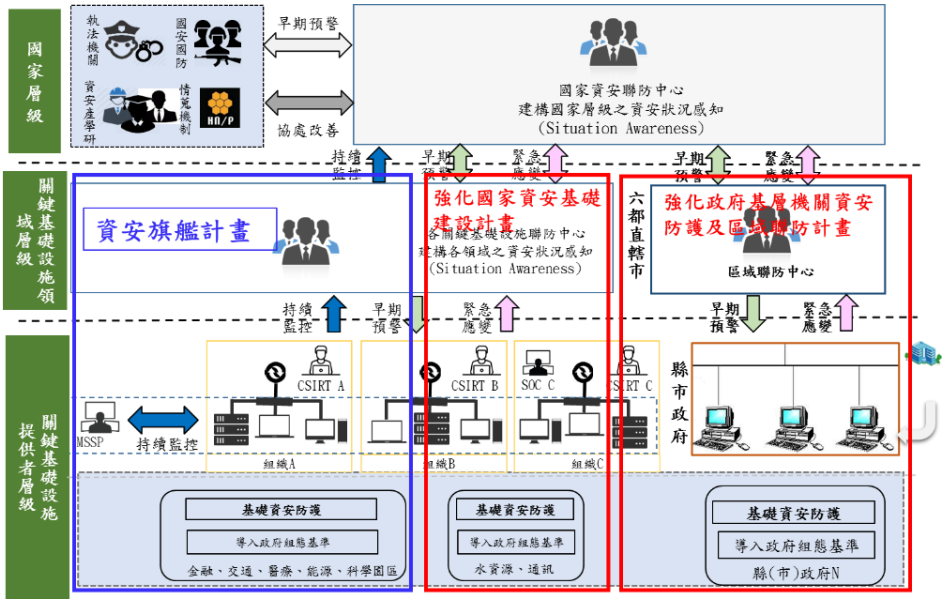
時程	累計預定進度(%)	關鍵查核點
108Q2	30%	完成 CNSPC 備援機房、NOMC 擴充案、C-ISAC 擴充案採購規格澄清及進行採購程序 完成佈點主機新增功能開發需求書
108Q3	60%	完成設備採購作業程序，設備到貨安裝及測試中 進行系統建置與客製化需求開發 完成 UL2900 確認及簽署合作契約
108Q4	100%	完成驗收、整合性試運行及驗收 繳交技術報告 依績效指標完成業者數目介接

109 年度預定進度

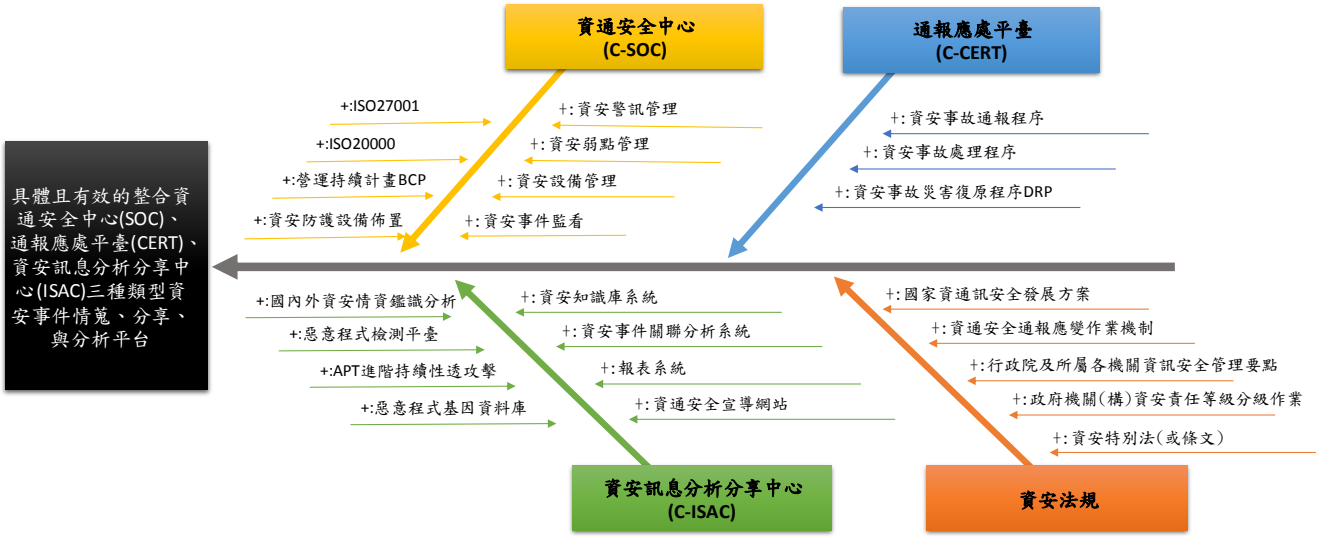
時程	累計預定進度(%)	關鍵查核點
109Q2	30%	NOMC 擴充案、C-ISAC 擴充案採購規格澄清及進行採購程序
109Q3	60%	完成設備採購作業程序，設備到貨安裝及測試中 進行系統建置與客製化需求開發 取得 UL 實驗室授權
109Q4	100%	完成驗收、整合性試運行及驗收 提供國內物聯網設備廠商檢測服務 依績效指標完成業者數目介接與業者輔導

四、重要科技關聯圖例

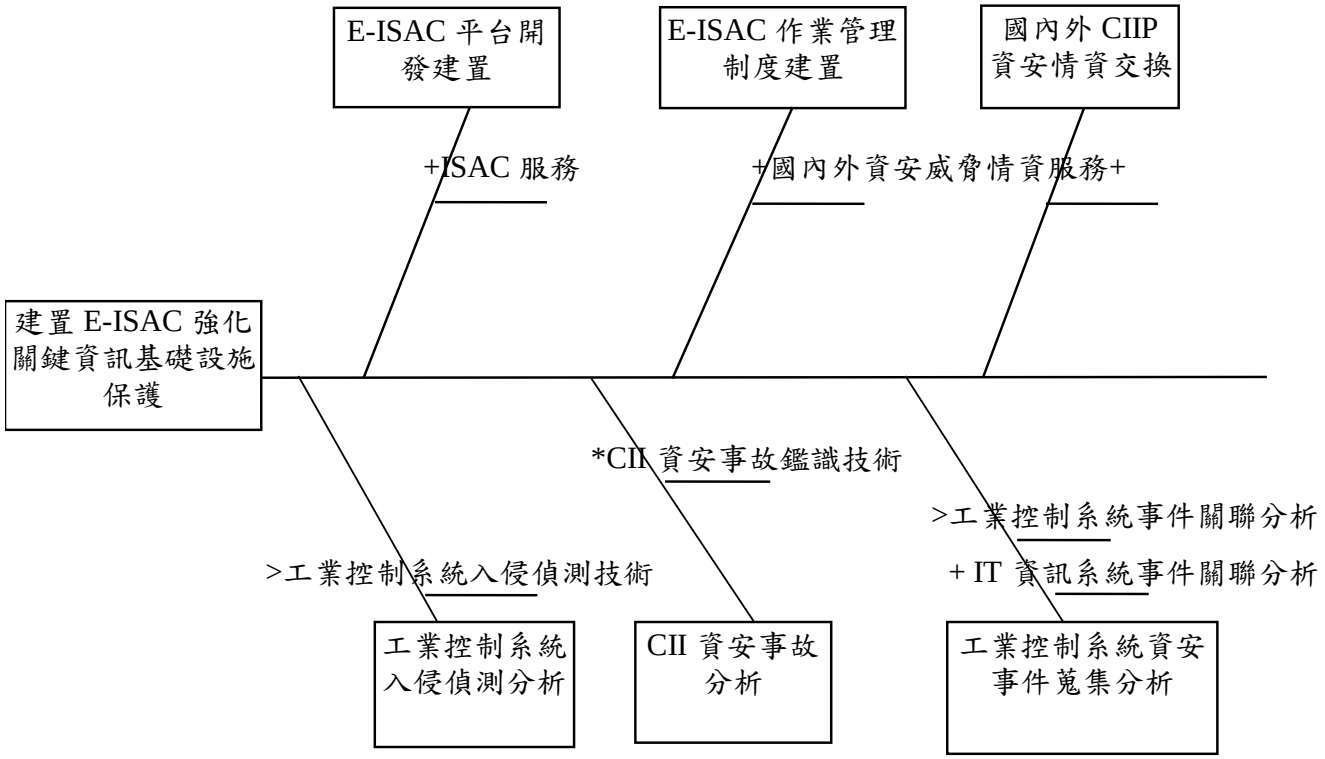
依據本院「國家資通安全發展方案(106年至109年)」發展策略，本計畫與本處另兩項計畫：「強化政府基層機關資安防護及區域聯防計畫」及「資安旗艦計畫」，共同落實「建構國家資安聯防體系、提升整體資安防護機制、強化資安自主產業發展」之目標，從風險管理的角度推動國家整體資安防禦工作，完成國家層級ISAC、CERT及SOC之建構，以達資安事件早期預警、持續監控、緊急應變、協處改善之目標，詳如下圖：



- 通傳會重要科技關聯圖如下：



- 經濟部重要科技關聯圖如下：



(註) 科技成熟度之標註：

＋：我國已有之產品或技術

＊：我國正發展中之產品或技術

＞：我國尚未發展中產品或技術

產品或技術若與「智慧財產權」有關亦請加註說明

參、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	-	107 年度完成 E-ISAC，服務範圍包括：公民營油、氣、電等領域，績效指標將在資安旗艦計畫呈現，預計服務 5 家業者	108 年度於本計畫將擴充水資源領域及經濟事務財團法人，預計服務擴增至 10%	109 年度服務擴增至 30%	經濟部關鍵資訊基礎設施領域之 E-ISAC、E-CERT、E-SOC 及 W-ISAC、W-CERT、W-SOC
		-	通傳會規劃於 107 年完成六大關鍵基礎設施領域業者之	108 年完成 80% 業者之收容與介接	109 年完成 100% 業者介接	通傳會關鍵資訊基礎設施領

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
			納管與通報，包含有：行動通信、固定通信、衛星通信、有線電視 SO、國際海纜及 DNS 網域，完成資料蒐集之定義及蒐集方式，後續將針對分析模組進行擴建			域之 ISAC、CERT、SOC
		-	1 份	1 份	1 份	提供通傳事業與水資源領域之資安事件分析及分享與鑑識服務，預計每季提供分析報告一份
		-	1 項	1 項	1 項	實測推薦我國資安優質產品(項)
			10%	25%	50%	其他設備採購國內自主產品

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，結合交通部、衛福部、經濟部及科技部、金管會等計畫，建立跨領域資安情報分享機制，強化關鍵基礎設施之資安分享與應變防禦能力。目標為建立重要關鍵資訊基礎設施領域之資安資訊分享及分析中心(ISAC)、資安通報應變中心(CERT)及資安監控中心(SOC)，共同強化資安情資縱向通報與橫向協防機制，以掌握國家整體資安風險。

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

本計畫建置經濟部與通傳會之關鍵資訊基礎設施領域之資安資訊分享與分析平台，並透過國家資安情資分享中心(N-ISAC)與其他領域 ISAC 平台串接，以降低資安事件衍生之風險，保障我國重要基礎設施之資通安全與人民權益。

另本計畫以使用國內資安產品達 50%為主要目標，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

本計畫由經濟部及通傳會統籌執行，非涉及競爭性計畫。

柒、其他補充資料

附件 1：經濟部

附件 2：通傳會

捌、106 年前瞻基礎建設計畫執行情形(截至 106/12/31)

本計畫為 107 年 1 月 1 日開始執行，截止 107 年 6 月辦理情形：

一、經濟部

年度	階段性目標達成情形	重要成果摘要說明
107 年(截至 6 月)	**分項一：建置關鍵基礎設施安全防護計畫(水資源)** 1. 強化水資源關鍵基礎設施資安防護能力。 2. 水資源領域 ISAC 資料交換規劃與 CERT 資料擷取平台建置。 **分項二：濟部關鍵資訊基礎設施資安資訊分享與分析平台計畫** 1. E-ISAC 平台開發建置。 2. 建置與經濟部關鍵基礎設施提供單位 ISAC 及 N-ISAC 介接介面。 3. 建置經濟部關鍵資訊基礎設施威脅燈號。	**分項一：建置關鍵基礎設施安全防護計畫(水資源)** 1. 完成「研擬 SCADA 資訊安全與入侵偵測方法」之相關資料蒐集。 2. 完成「W-ISAC 資料交換介面需求規格書」。 3. 完成「W-ISAC 資料交換介面設計規格書」。 4. 完成「水資源領域之安全研究」。 5. 完成「資訊資產盤點與風險評估之各水庫訪談作業」3 次。 **分項二：經濟部關鍵資訊基礎設施資安資訊分享與分析平台計畫** 1. 完成 E-ISAC 平台系統規劃，包括系統分析報告書、系統設計報告書及系統測試計畫書。 2. 完成經濟部及所屬資安資訊分享與分析平台(ISAC)介接研商會議。

		3. 完成 E-ISAC 平台之強化資安環境硬體設備採購。 4. 完成關鍵資訊基礎設施威脅燈號蒐集及研究，並確認經濟部威脅燈號規劃方向。

二、國發會

年度	階段性目標達成情形	重要成果摘要說明
107 年(截至 6 月)	1. 建置專屬資訊安全監控中心 2. 建立 DNS 服務系統 3. 建置巨量資料分析平臺	1. 資訊安全監控中心已收容閘口 IPS、接取端 IPS、路由器 syslog 以及 DMZ 區防火牆等，每日分析高達 4300 萬筆日誌，目前已運用關聯分析技術找出高度關注風險事件達 331 件。 2. DNS 快取系統僅提供 GSN 用戶進行網域查詢，每日受理超過 2 億次查詢，同時防止外部惡意存取本關鍵基礎服務。另外本系統架設安全設備，抑止惡意攻擊，並結合黑白名單機制，避免用戶連結至惡意網站，目前已防堵超過 6 億次惡意查詢。同時設置異地 2 套 DNS 網域查詢服務，確保高穩定性 DNS 查詢基礎服務。 3. 巨量資料分析平台透過大數據分析每日處理 2 億筆之 DNS 查詢紀錄以及 20 億筆 Proxy Log，藉由巨量資料運算能力與數學統計應用，專注在網路攻擊的控制及擴散行為的偵測。目前已找出超過 3 萬筆可疑活動，並發現 293 個 GSN IP 有異常行為，並辨識出 178 個惡意網域名單。同時已經辨識出惡意網域名單回饋至相關安全防護設備上進行阻檔，並執行告警。

三、通傳會

年度	階段性目標達成情形	重要成果摘要說明
106 年	於科發基金補助之 106 年資安旗艦計畫建置完成 C-SOC	1. 完成資安監控平台 C-SOC 建置，並進行 7*24 小時資安事件即時監控。 2. 完成垃圾郵件暨資安事件分析管理平台建置。 3. 完成本會與 N-ISAC 以新一代 STIX 交換格

		式雙向界接，並取得及分析資安情資。
107 年(截至 6 月)	完成新一代資安監控平臺(C-SOC)高雄第二監控中心建置，及新一代資訊分析與分享平臺(C-ISAC)、資安通報應變平臺 (C-CERT)建置。並完成與 12 家通傳事業雙向介接。	4. 擴增通傳事業佈點主機及垃圾郵件之誘捕系統：年度績效指標預計完成 12 家業者佈點主機擴建，尚餘 5 家業者需透過預算解凍來協助建置。 5. 建置新一代資安監控平臺(C-SOC)高雄第二監控中心及新一代資安監控平臺系統效能監控建置：已於 5 月 15 日辦採購公告、6 月 7 日開標、6 月 28 日決標，預計將於 8 月底完成整體建置。 6. 「新一代資訊分析與分享平臺暨惡意程式檢測系統」建置案已於 5 月 15 日辦理公告並於 6 月 4 日開標、6 月 28 日決標，刻正與廠商討論完成系統架構與設計之規劃。 7. 「資通安全暨防制垃圾郵件濫發宣導網站」建置案已於 5 月 15 日辦理公告並於 5 月 29 日開標、6 月 25 日決標。刻正與廠商、通傳會討論及確認網站架構再進行後續開發。整體建置預計於 11 月底前完成。

附件 1

前瞻基礎建設－數位建設

強化國家資安基礎建設之分項計畫

經濟部

107 年 8 月

經濟部關鍵基礎設施安全防護計畫

一、計畫緣起

關鍵基礎設施(Critical Infrastructure, CI)建立之目的是國家為了維持民生、經濟與政府等相關運作所需之基本設施與服務，包括實體及以資訊電子為基礎之系統，為重要社會基礎功能所需之基礎建設，諸如：公民營電信、電力、能源、金融、醫療、交通、緊急救助等。各種關鍵基礎設施系統，只要牽涉到設備連網，加上採用開放技術架構，都會讓關鍵基礎設施面臨資安風險，相關單位應透過各種資訊分享方式，做到資安事件的提前預警。

由於許多關鍵基礎設施之系統監控和資料擷取系統(以下簡稱SCADA)有遠端操控系統需求，採用開放的連網架構，國外也陸續傳出各式針對工業控制系統的資安威脅與攻擊事件。根據美國國土安全部(DHS)所屬的工業控制系統緊急應變小組(Industrial Control Systems Cyber Emergency Response Team, ICS-CERT)針對美國石油、水力設施、電廠等關鍵基礎設施之統計，在 2016 年總共處理 390 個通報事件，其中有 186 個是來自於關鍵基礎設施的事件，屬能源設施有 41 個事件，水和污水系統設施則有 83 個事件。此外，ICS-CERT 所處理的系統弱點協調工作數量，近年來也有增加趨勢，**自 2016 年的 363 件成長至 2017 年的 568 件，成長幅度約 56%**。然而知名隱私暨資訊管理研究機構 Ponemon Institute 最近為西門子公司所執行之研究「了解石油和天然氣行業的公司如何解決運營技術（OT）環境中的網絡安全風險」中，發現於 OT 所有網路攻擊中，46%的攻擊發生時並未被業主發現，由此數據顯示 OT 環境之網路攻擊風險日益提高。

另根據 Ahu Dhabi 會議組織的數據顯示，2016 年石油和天然氣公司領導人以及行業認證機構 DNV GL 報告了近 100 次網絡攻擊，估計網絡犯罪對於能源和公用事業造成的商業損失和設備損壞約為 1,280 萬美元。近期**勤業眾信**(Deloitte)針對 2017 年發布的報告中也指出石油和天然氣行業

將面臨日益嚴重的網路攻擊風險，因此強化關鍵資訊基礎設施防護勢在必行。

二、計畫目標

鑒於經濟部主管之能源與水資源關鍵基礎設施之數位化工業控制系統資通安全需求，在「資安即國安」之國家政策方針下，依據「數位國家・創新經濟發展方案」及「第五期國家資通安全發展方案 (106 至 109 年) 」策略，規劃「打造安全可信賴的數位經濟時代」及「建置國家資安機制，提升自我防護能量」，經濟部擬定「經濟部關鍵基礎設施安全防護計畫」，除了強化水資源關鍵基礎設施之安全外，亦開發建置經濟部關鍵資訊基礎設施(Critical Information Infrastructure, CII)資安資訊分享與分析平台(Economic CII Information Sharing and Analysis Center，以下簡稱 E-ISAC)，並透過國家資安情資分享中心(N-ISAC)與其他領域 ISAC 平台串接，以建立跨領域聯防機制。108 年至 109 年將建置並精進經濟部資安事件緊急應變平台與通報機制(Economic/Water - Computer Emergency Response Team，以下簡稱 E/W-CERT)，強化之資安事件之通報、應變處理能力與管理，以及建立經濟部二線資訊安全監控中心(2nd Line - Security Operation Center, 以下簡稱 E/W-SOC)，為關鍵資訊基礎設施之整體資安防護奠定基礎，並將參考如美國國土安全部 NCCIC 及 ICS-CERT 等之 OT 領域相關資通安全作法，以提升能源與水資源領域關鍵基礎設施之資通安全。主要目標如下：

(一)強化水資源關鍵基礎設施資安防護，防範水資源關鍵資訊基礎設施免於遭受資安攻擊之風險，提升水資源關鍵基礎設施提供機關資訊基礎環境之安全性及穩定性。

1.持續擴充 W-ISAC 功能與情資以達資安資訊分享。

2.建置 W-CERT 平台以作為關鍵基礎設施資安事件通報機制之基礎，藉此強化各水庫、堰、壩關鍵基礎設施同仁資安意識。

3.經濟部水利署本部已導入 SOC 監控維運，並規劃自 108 年度起各水資源局、河川局陸續導入 SOC 監控維運，建立一線 SOC 之基礎，於 109 年建置 W-SOC(二線 SOC)，以建立經濟部水利署資安聯防機制，提升資安預警能力。

(二)透過建置資安資訊分享及分析(E/W-ISAC)平台、資安通報應變中心(E/W-CERT) 平台、二線資安監控中心平台(E/W-SOC)平台，建立關鍵資訊基礎設施資安聯防機制，為整體關鍵基礎設施之資安防護奠定基礎，降低資通安全風險對關鍵基礎設施運作之影響。

三、計畫內容與實施策略

(一)分項計畫一：建置關鍵基礎設施安全防護計畫(水資源)

1.計畫架構：

經濟部水利署係兼具水資源開發、管理及河川管理之多重角色機關，相關水資源關鍵基礎設施操作及資料使用相對重要，如何避免 921 地震、815 大停電、颱風豪雨及網路攻擊所產生資安風險，及降低無預警災害衝擊，以達成不中斷資訊服務，為資安管理重要之一環。為達成前述目標，當從備援機制、異地備份、災害復原機制及作業制度等多方面建立技術範疇，期許經濟部水利署及所屬機關資訊系統於因人為、天災及網路攻擊導致運作停頓時，可由備援中心及時接替作業，使資訊服務不中斷。

經濟部水利署於 107 年度建置「水資源領域資安資訊分享與分析平台 (W-ISAC)」之架構與應用系統，以及「水資源領域資安事件緊急應變平台(W-CERT)」之雛形。108 年及 109 年將持續擴充「水資源領域資安資訊分享與分析平台」之功能與軟硬體設備，其相關軟硬資訊設備將研擬於經濟部水利署與新北市政府聯合新建的安坑輕軌捷運 K8 站(本工程列入前瞻基礎建設-軌道交通建設之一)水利大樓資訊機房佈建。另將建立經濟部水利署 W-SOC 二線平台，導入二線資安監控

與擴充，並建置 W-CERT 緊急應變組織、職掌及作業程序，以強化資安事故發現能力，逐步監控水庫水資源領域相關產業鏈並提供監控及情資分享，此外亦將進行經濟部水利署及所屬機關之資料備份及系統備援，強化保護資料安全能力，降低人為及天災造成資料損毀的風險。另依專家建議盤點既有之水工機械及電控相關設備，並將參酌 SIL(Safety Integrity Level)之安全完整性標準，評估相關設備進行智慧管理化之可行性。

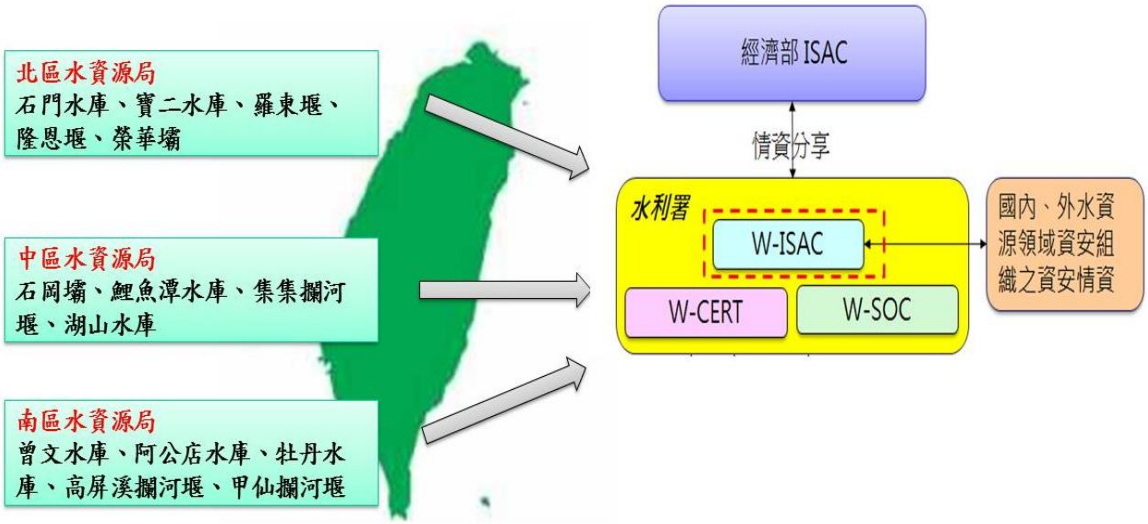


圖 1 水資源關鍵基礎設施防護規劃架構圖

計畫說明：

本計畫主要是推動水資源關鍵資訊基礎設施之防護規畫，藉由上述架構，強化水資源關鍵基礎設施資安防護能力。經由持續擴充 W-ISAC 功能與情資以達資安資訊分享，並完備 W-CERT 平台與水資源領域 W-CERT 制度，以作為關鍵基礎設施資安事件通報機制之基礎。持續推展關鍵基礎設施資訊資產盤點與風險評估工作，並研擬「水資源領域關鍵基礎設施資安防護政策與基準」，以作為各水庫單位維運關鍵基礎設施之資安防護指引。經由教育訓練與推廣活動，提高 IT 及 OT 專長領域同仁之資安意識，強化各水庫、堰、壩關鍵基礎設施整體資訊安全。

2.工作項目：

108 年至 109 年計畫工作項目：

(1)水資源關鍵資訊基礎設施防護監控範圍擴充與延伸整備

使用適合水資源關鍵資訊基礎設施資安防護之軟硬體設備，以增強資安防護能力。此外，透過資安事件攻擊演練，了解與評估現行資安防護程序、人員、技術之完備情形，並進行後續改善作業規劃與實施。

(2)完備 W-CERT 平台功能並建立 W-CERT 制度

以 107 年度建置之 W-CERT 雛型為基礎，完備 W-CERT 在身分驗證、存取控管、事件通報、事件處理、會員資料維護及通報演練等方面之功能，並規劃**水資源需通報之資安事件**的定義、重要等級，成為實際可運行之平台。

於平台功能完備之後，將建立水資源領域 W-CERT 制度，結合水資源關鍵資訊基礎設施資安事件應變機制，以強化資安事件之通報、應變處理能力與管理。

平台與制度建置相關技術，亦將於此工作項目之執行過程中一併轉移。

(3)W-SOC 二線平台之規劃與建置

成立 W-SOC 二線平台，以自動化方式將經濟部水利署一線 SOC 資安警訊通報與相關事件傳送至 W-SOC 二線平台。於 W-SOC 二線平台 7x24 監控管理與監看資安事件，並透過 W-SOC 二線平台關聯規則進行資安監控通報事件交叉分析，當發現資安事件之徵兆或資安警訊時，可立即分析與處理，可更有效彙整經濟部水利署資安監控事件，找出資安事件之發生原因以及研擬防範措施，並發揮資安事件先兆事件之預警機制，以期降低資安事件可能造成之損失。W-SOC 二線平台與主管機關經濟部二線 SOC 平台介接，將相關資安

監控通報事件傳送至經濟部二線 SOC 平台，以強化資安聯防體系。

W-SOC 平台功能如下：

A.SOC 資安事件單與關聯事件紀錄收集機制

以自動化方式收集水資源領域之各機關一線 SOC 資安通報事件單與關聯事件紀錄，涵蓋 IT、OT 資安事件，並於 W-SOC 平台系統設計自動化規則進行事件分類與分級。

B.資安聯防監控機制

於 W-SOC 平台綜合分析水資源領域關鍵基礎設施各機關之 SOC 資安事件單與關聯事件紀錄，進行整體威脅趨勢分析及國內外威脅來源分析，彙整成資安情資，提供回饋建議、資安防禦之資訊予轄管機關，以利各機關及早準備因應，達到資安聯防效果。

C.資安事件情蒐分析

依據前述 W-SOC 平台之事件分類、分級結果，與國內、外水資源領域資安情資綜整分析，獲得水資源領域整體資安威脅趨勢之情資以供分享。

D.E-SOC 資訊介接

W-SOC 平台將與經濟部 E-SOC 平台進行資訊介接，建立資訊回傳機制，除針對緊急事件進行資訊回傳，並可針對相關威脅情資所關聯發現之重要資安情資進行聯防預警通知，以達經濟部體系資安威脅綜整分析與聯防機制之用。

E.領域聯防情資回饋

W-SOC 平台根據下轄機關 SOC 所回傳之資安通報事件單與關聯事件紀錄進行彙整、分析，提供各類聯防回饋情資，以供進行聯防偵測與防護。回饋情資包含情資來源單位、資安威脅類別、威

脅來源國家別及惡意程式種類、入侵攻擊指標資訊(Indicator of Compromise, IoC)等。

F.技術移轉

W-SOC 平台建置相關技術，亦將於此工作項目之執行過程中一併轉移。

(4)水資源關鍵資訊基礎設施風險控管強化

經濟部水利署 108 年度的資訊資產盤點,係延續 106 年度及 107 年度的計畫，擴大資訊資產盤點的範圍，並包括 OT 設施與系統的部分。經濟部水利署 106 年度的資訊資產盤點主要範圍為北區水庫單位，107 年度則為中區水庫單位，108 年度則為南區水庫單位。並且針對已實施之範圍進行風險再評估，以作為持續了解資安相關威脅與風險，並據以擬定具體改善計畫與實施改善措施。

此外，將蒐集、研析國內外對水資源領域關鍵基礎設施之資安防護政策與基準，增訂適合我國水資源領域資安防護政策與基準，以作為各水庫單位維運水資源關鍵基礎設施之資安防護指引，據以實施定期資安稽核、資安演練，以及進行資安縱深防護，使得業務持續運作穩定。

(5)規劃與輔導建置工業控制系統資訊安全與入侵偵測平台實驗環境

參考國際工業控制安全標準（ISA-99/IEC 62443），進行水資源領域關鍵基礎設施相關工業控制系統之安全性研究，同時運用入侵偵測系統之偵測概念，研究相關工業控制系統之安全，訂定系統安全需求與安全等級之依據。

(6)水資源領域威脅燈號調整及與經濟部威脅燈號介接

持續蒐集國、內外資安相關資訊、標準，配合國內水資源領域關鍵基礎設施現況進行調整。檢視威脅燈號相關構面、評估問項、

基準值、級距等，進行威脅燈號系統重新評估與調整，更新威脅燈號系統，以期更能反應水資源領域之威脅現況，以利主管與相關管理人員及時掌握與判斷威脅情形，及時採取適當之防範或防護措施。另亦將水資源領域之威脅燈號與經濟部威脅燈號介接，將水資源領域之威脅等級相關數據以自動化方式傳送至經濟部，以利上級主管能掌握水資源領域之威脅情形。

(7)資料備份備援中心規劃建置

採整體規劃設計與建置，並與現行台中辦公區資訊機房、台中文心 IDC 機房及所屬機關得以互相通訊。規劃機櫃系統、網路佈線、不斷電系統、空調設備、機房環控系統等相關設施，期使設備完善、網管安全效能及緊急應變支援目標。

(8)強化水資源關建基礎設之基礎資通環境安全

為強化水資源關建基礎設之基礎資通環境安全、資安雲端智能分析平台及閘道威脅安全防護，將引進以下方案：

A.網路攻擊分析、偵測與防禦

B.APT 防禦

C.DDoS 防禦

D.網頁/主機弱點防範

(二)分項計畫二：經濟部關鍵資訊基礎設施資安資訊分享與分析平台計畫

1.計畫架構：

本計畫主要是藉由資安資訊分享及分析(E-ISAC)平台、資安通報應變中心(E-CERT) 平台、二線資安監控中心平台(E-SOC)平台，並與所屬機關(構)單位及國家層級 N-ISAC、N-CERT 及 N-SOC 合作介接進行情資交換及通報，強化整體水資源及能源資安防禦與應變措施，全

程計畫規劃架構如下圖所示：

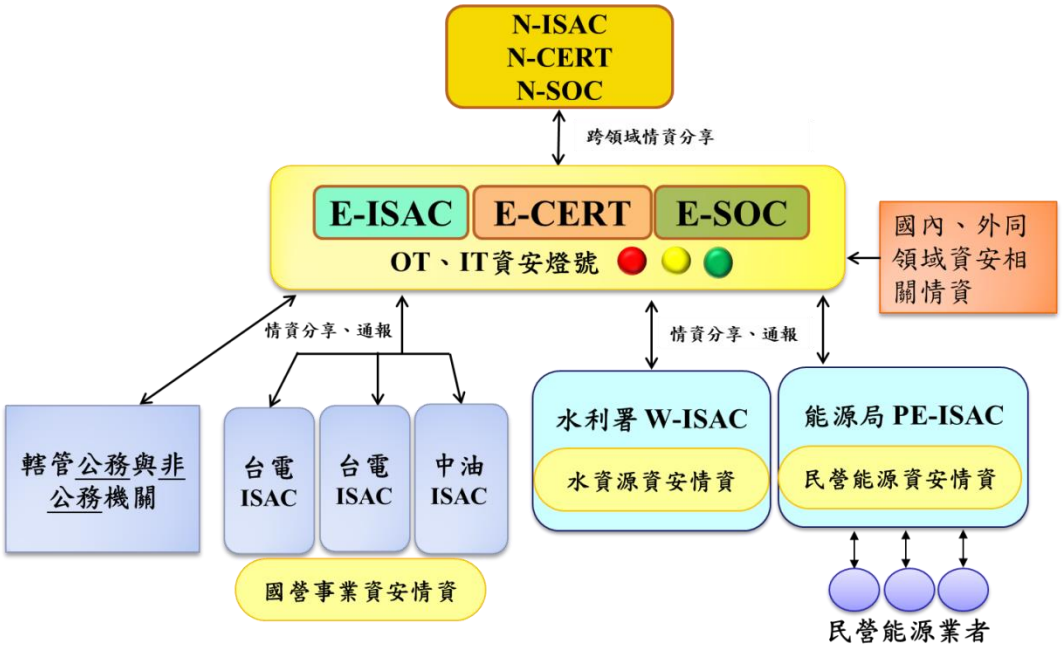


圖 2：經濟部 E-ISAC、E-CERT、E-SOC 平台計畫整體架構

2.計畫說明：

經濟部於 107 年度建置 E-ISAC 系統，除了與上層 N-ISAC 情資交換介接，並與所屬機關以及國營事業單位之 ISAC 平台資料交換介接，包括 PE-ISAC、W-ISAC，以及中油公司、台電公司、台水公司之 ISAC 平台交換介接，初步達成資安情資分享的目標。

108 年至 109 年將持續擴充 E-ISAC 平台，建立經濟部所屬公務機關、特定非公務機關之資安聯防體系，並建置 E-CERT 平台、E-SOC 平台，建立處理資安事件之事前、事中與事後之作業程序，以期降低資安事件所造成之損失，強化資安通報事件應變能力，落實聯防機制以提升資安防護能力。

3.工作項目

108 年至 109 年計畫工作項目：

(1)**擴充建置 E-ISAC 情報資料庫**

持續蒐集國內外資安機構資安情資,包括與 W-ISAC、PE-ISAC、國營事業 ISAC 介接分享之 OT 資安情報，並建立情資分析審查機制，邀集領域專家針對重大情資，挑選必要性與重要性議題進行進階分析、研判，強化資安情資的深度，提供 ISAC 會員掌握資安防護之最新訊息，以擴充資安情資並進行資安情資分析與分享。規劃

(2)**擴充 E-ISAC 平台服務範圍**

除原先加入服務範圍之經濟部水利署、經濟部能源局、中油、台電及台水外，將擴大納入經濟部所轄管公務、特定非公務機關(含公營事業及政府捐助財團法人)為平台會員，以建立完整之資安防護體系。

(3)**建置 E-CERT 平台**

經由建置 E-CERT 平台與實施資安事件通報緊急應變機制，掌握經濟部所屬能源領域、水資源領域之特定非公務機關等資安通報事件，透過自動化平台提供完備之通報機制，強化緊急應變與處置作業，以降低資安事件發生時所伴隨之損害，在最短時間內儘速恢復正常營運。

定期綜整通報事件來源、事件類型與處理情形，追蹤了解特定非公務機關事件處理情形，確保資安事件處理完善。另為因應經濟部所轄能源領域、水資源領域關鍵基礎設施與下屬機關所發生、通報之資安事故,E-CERT 需成立緊急應變組織、建立緊急應變相關職責及作業程序，包括資安事故分類分級與通報、資安事故處理諮詢協助、資安訊息發布(含緊急情資通報)、資安認知宣導服務等。

E-CERT 平台功能包含：

A.身分驗證與存取控管

E-CERT 通報平台將規劃帳號管理與身分識別機制。

B.事件通報

建立自動化系統，提供特定非公務機關發現資安事件時，可配合填寫通報，並提供多種通報管道。透過審核流程，以即時掌握轄管單位資安現況追蹤資安事件原因、處理進度及損害範圍。

C.事件處理

E-CERT 設置諮詢管道，提供防護建議及相關事件處理建議，協助特定非公務機關進行事件處置，媒合技術團隊提供技術支援。

D.特定非公務機關資料維護功能

建立通報帳號申請管道，並定期確認特定非公務機關聯絡資料正確性與完整性，落實登錄情形以完善通報機制。

E.通報演練功能

提供系統演練功能以查核 E-CERT 後執行狀況，演練項目包含通報演練及事件處理情境演練，前者確認 E-CERT 通報聯繫管道暢通及強化人員了解通報作業，後者則確認事件處理人員了解事件處理程序。

F.網站訊息公告

公告 E-CERT 重要訊息，以提供會員參考及注意。

G.技術移轉

E-CERT 平台建置相關技術，將於此工作項目之執行過程中一併轉移。

(4)建置 E-SOC 平台

建置 E-SOC 監控情蒐中心，以自動化系統收集能源領域、水資源領域之特定非公務機關自建或委外 SOC 之資安事件單與關聯事

件紀錄，彙整 IT、OT 資安情資以及防護狀況，進行資安情資風險判定及決策支援，並將資安情報定期報告行政院資通安全處及通報各機關 SOC 進行協防，以減低機關資安威脅，掌握領域整體資安現況及趨勢，以期達成事前防範與資安聯防之綜效。E-SOC 平台功能如下：

A.SOC 資安事件單與關聯事件紀錄收集機制

以自動化方式收集能源、水資源領域之各機關 SOC 資安通報事件單與關聯事件紀錄，涵蓋 IT、OT 資安事件，並於 E-SOC 平台系統設計自動化規則進行事件分類與分級。

B.資安聯防監控機制

於 E-SOC 平台綜合分析經濟部轄下能源與水資源領域關鍵基礎設施各機關 SOC 資安事件單與關聯事件紀錄，進行整體威脅趨勢分析及國內外威脅來源分析，彙整成資安情資，提供回饋建議、資安防禦之資訊予經濟部轄管機關及特定非公務機關，以利各機關及早準備因應，達到資安聯防效果。

C.資安事件情蒐分析

依據前述 E-SOC 平台之事件分類、分級結果，與國內、外能源與水資源領域資安情資綜整分析，獲得能源與水資源領域整體資安威脅趨勢之情資以供分享。

D.N-SOC 資訊介接

E-SOC 平台將與 N-SOC 平台進行資訊介接，建立資訊回傳機制，除針對緊急事件進行資訊回傳，並可針對相關威脅情資所關聯發現之重要資安情資進行聯防預警通知，以達國家整體資安威脅綜整分析與聯防機制之用。

E.領域聯防情資回饋

E-SOC 平台根據下轄機關 SOC 所回傳之資安通報事件單與關聯事件紀錄進行彙整、分析，提供各類聯防回饋情資，以供進行聯防偵測與防護。回饋情資包含情資來源單位、資安威脅類別、威脅來源國家別及惡意程式種類、入侵攻擊指標資訊(Indicator of Compromise, IoC)等。

F.**技術移轉**

E-SOC 平台建置相關技術，將於此工作項目之執行過程中一併轉移。

(5)**訂定 E-CERT 作業規範**

為確保於知悉資通安全事件時，迅速進行通報及進行適當之應變，本計畫將訂定作業規範，包括

A.判定事件等之流程及權責

B.事件之影響範圍、損害評估及機關因應能力之評估

C.資通安全事件之內部通報流程

D.通知受資通安全事件影響之其他機關之方式

E.通報演練方式

F.資通安全事件通報窗口及聯繫方式

G.應變小組之組織

H.事件發生前之防護措施規劃、演練及資通安全資訊偵測作業

I.事件發生時之損害控制機制

J.事件發生後之復原、鑑識、調查、及改善機制

K.事件相關紀錄之保留

L.其他資通安全事件通報、應變相關事項

(6)**訂定 E-SOC 作業規範**

建置 E-SOC 之作業管理制度文件,提升專案成員相關 E-SOC 制度與管理能力及預防監督可能發生之資訊風險，以完備 E-SOC 管理制度，使 E-SOC 得以持續順暢運作。

四、實施範圍

實施對象：經濟部轄管公務機關、特定非公務機關，經濟部水利署下屬機關
實施區域：北區、中區、南區

五、計畫期程

108 年 1 月 1 日至 109 年 12 月 31 日止。

六、關鍵績效指標

(一) 108 年度

1.完成 E-CERT 平台建置

2.完成 W-CERT 平台建置

(二) 109 年度

1.完成 E-SOC 平台建置

2.完成 W-SOC 平台建置

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,「經濟部關鍵基礎設施安全防護計畫」以關鍵資訊基礎設施之整體資安防護，提升能源與水資源領域關鍵基礎設施之資通安全，為維持民生、經濟與政府運作的重要工作之一，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)建置關鍵基礎設施安全防護計畫(水資源)

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		
108	1	完備 W-CERT 平台功能並建立 W-CERT 制度	完備 W-CERT 平台功能建立 W-CERT 制度		5,000,000	W-CERT 制度實施範圍包括經濟部水利署與北中南水資源局	1
	2	W-SOC 一線平台中心之規劃與導入	規劃與導入北中南水資源局 W-SOC 一線平台中心及日誌儲存系統		8,100,000	W-SOC 一線平台中心之規劃與導入	2
	3	水資源關鍵資訊基礎設施風險控管強化	水資源關鍵資訊基礎設施資訊資產盤點與風險評估。研擬水資源領域資安防護政策與基準。		3,200,000	● 風險評估實施範圍包括南區水資源局及水庫堰壩單位。 ● 風險再評估實施範圍包括北區水資源局及所轄水庫單位；中區	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
				經常門	資本門		
						水資源局及所轄水庫單位	
	4	規劃與輔導建置工業控制系統資安防護與入侵偵測平台實驗環境	規劃與輔導建置工業控制系統資安防護與入侵偵測平台實驗環境		2,600,000	完成規劃報告	4
	5	資料備份備援中心規劃建置(第一階段)	規劃設計資料備份備援中心整體架構，建立資料備份備援先期環境		8,600,000	完成規劃設計報告及備份備援架構及臺北辦公區部分資訊系統完成備份備援測試及監控運作情形	5
	6	強化水資源關建基礎設之基礎資通環境安全	● 網路攻擊分析、偵測與防禦 ● APT 防禦 ● DDoS 防禦		12,500,000	● 確保全年無重大資安事件 ● 資安設備更新 ● 內部威脅阻絕	6

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		
			● 網頁/主機弱點防範				
109	1	ISAC 功能擴充整備	水資源關鍵資訊基礎設施防護監控範圍擴充與延伸整備。		2,400,000	● ISAC 平台功能擴充與精進 ● 實施廠區演練	1
	2	W-SOC 二線平台建置	W-SOC 二線平台建置		2,100,000	W-SOC 二線平台	2
	3	W-CERT 平台功能擴充	W-CERT 平台強化資訊安全防護		2,000,000	W-CERT 平台強化資訊安全防護	3
	4	水資源關鍵資訊基礎設施風險控管強化	水資源關鍵資訊基礎設施風險評估		2,750,000	實施範圍包括北中南水資源局	4
	5	規劃與輔導建置工業控制系統資安防護與入侵偵測平台實驗環	於平台實驗環境進行測試，並完成測試報告		800,000	於平台實驗環境進行測試，並完成測試報告	5

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		
		境					
	6	資料備份備援中心規劃建置(第二階段)	建立網路安全管理、軟硬體相關設施、機房監控環境及緊急應變處理能力		17,750,000	與現行臺中辦公區資訊機房、台中文心 IDC 機房互相備份備援及全面監控系統運作情形	6
	7	強化水資源關建基礎設之基礎資通環境安全	● 網路攻擊分析、偵測與防禦 ● APT 防禦 ● DDoS 防禦 ● 網頁/主機弱點防範		12,200,000	● 確保全年無重大資安事件 ● 資安設備更新 ● 內部威脅阻絕	7
合計				80,000,000 元			

（二） 經濟部關鍵資訊基礎設施資安資訊分享與分析平台計畫

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		
108	1	擴充建置 E-ISAC 情報資料庫	提供 ISAC 會員掌握資安防護之最新訊息		3,000,000	廣泛收集國際資訊、情資經整理、分析從中萃取出資安情資並定期發佈	4
	2	擴充 E-ISAC 平台服務範圍	將擴大納入經濟部所轄管公務、特定非公務機關		3,000,000	ISAC 平台功能擴充與精進	3
	3	建置 E-CERT 平台	E-CERT 平台與實施資安事件通報緊急應變機制並強化平台所在之環境安全		12,000,000	E-CERT 制度實施範圍經濟部所屬能源領域、水資源領域之特定非公務機關	1
	4	訂定 E-CERT 作業規範	訂定作業規範		2,000,000	確保於知悉資通安全事件時，迅速進行通報及進行適	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		
						當之應變	
109	1	擴充建置 E-ISAC 情報資料庫	提供 ISAC 會員掌握資安防護之最新訊息		3,000,000	廣泛收集國際資訊、情資經整理、分析從中萃取出資安情資並定期發佈	4
	2	擴充 E-ISAC 平台服務範圍	將擴大納入經濟部所轄管公務、特定非公務機關		3,000,000	ISAC 平台功能擴充與精進	3
	3	建置 E-SOC 平台	建置 E-SOC 監控情蒐中心，以自動化系統收集並強化平台所在之環境安全		12,000,000	建立 E-SOC 二線平台中心與實施維運作業	1
	4	訂定 E-SOC 作業規範	建置 E-SOC 之作業管理制度文件		2,000,000	完備管理制度，順暢持續運作環境	2
合計				40,000,000 元			

九、預定進度(建議參考計畫期程中的表格內)

(一)建置關鍵基礎設施安全防護計畫(水資源)

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%	4,000,000	完成 108 年度專案管理計畫書
108 年 7 月	50%	20,000,000	完成第二期報告
108 年 10 月	85%	34,000,000	完成第三期報告
108 年 12 月	100%	40,000,000	完成 108 年度期末報告

109 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
109 年 3 月	10%	4,000,000	完成 109 年度專案管理計畫書
109 年 7 月	50%	20,000,000	完成第二期報告
109 年 10 月	85%	34,000,000	完成第三期報告
109 年 12 月	100%	40,000,000	完成 108 年度期末報告

(二)經濟部關鍵資訊基礎設施資安資訊分享與分析平台計畫

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%	2,000,000	完成 108 年度專案管理計畫書
108 年 7 月	50%	10,000,000	完成第二期報告
108 年 10 月	85%	17,000,000	完成第三期報告
108 年 12 月	100%	20,000,000	完成 108 年度期末報告

109 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
109 年 3 月	10%	2,000,000	完成 109 年度專案管理計畫書
109 年 7 月	50%	10,000,000	完成第二期報告
109 年 10 月	85%	17,000,000	完成第三期報告
109 年 12 月	100%	20,000,000	完成 108 年度期末報告

十、預期效益

(一)擴充經濟部 E-ISAC、水資源領域 W-ISAC 資安情資分享平台之功能，強化資安防護訊息分享之自動化與有效性，完成與其他領域資安平台串接，以建立跨領域聯防機制。

(二)建置經濟部 E-CERT、與水資源領域 W-CERT 之資安事件應變平台及相關維運制度，強化資安事件應變處理能力與管理機制。搭配經濟部 E-SOC 與水資源領域 W-SOC 二線平台及相關維運制度之建置，可更有效彙整經濟部與經濟部水利署資安監控事件，找出資安事件之發生原因以

及研擬防範措施，並發揮資安事件之預警機制，以降低資安事件可能造成之損失，提升水資源領域關鍵基礎設施資安防護能力。

(三)建置水資源關鍵資訊基礎設施資安防護之軟硬體設備，以增強資安防護能力及完成宣導資安控制措施、教育訓練，交流 IT 與 OT 安全相關知識，使相關從業人員得以提升資安意識及技術能力。

(四)完成經濟部水利署北、中、南區水資源局及所屬單位關鍵資訊基礎設施進行資訊資產盤點與風險評估作業，並針對已實施之範圍進行風險再評估，以作為持續了解資安相關威脅與風險，並據以擬定具體改善計畫與實施改善措施，以強化整體資安防護能量。

(五)完成水資源領域資安防護政策與基準，作為水資源關鍵基礎設施相關單位依循之標準，並據以實施定期資安稽核、資安演練，以提升資安防護縱深，使業務得以持續穩定運作。

(六)提昇對於關鍵基礎設施安全保護相關議題之關注，進而加強水資源領域關鍵基礎設施各機關電腦網路系統、工業控制系統等安全防護機制，藉此降低資安事件發生的風險及潛在威脅。

十一、相關聯絡資料

(含單位、聯絡人姓名、電話、E-mail 等)

單位	姓名	連絡電話	電子郵件
經濟部	林淑媛	02-2321-2200 ext 8669	SYLIN2@moea.gov.tw
經濟部	陳永昌	02-2321-2200 ext 8687	ycchen5@moea.gov.tw
經濟部水利署	黃貴麟	04-22501419 ext 419	a210010@wra.gov.tw
經濟部水利署	何茂松	04-22501423 ext 423	a210050@wra.gov.tw

附件 2

前瞻基礎建設－數位建設

強化國家資安基礎建設之分項計畫

通傳會

107 年 8 月

數位匯流資通安全分析管理平臺建置與服務計畫

一、 計畫緣起

(一)政策依據

近年來，數位經濟帶動產業朝跨世代、跨境、跨領域、跨虛實等趨勢發展，促使全球產業格局翻轉。我國擁有厚實的工業基礎，面對數位經濟與物聯網(IOT)時代的來臨，建構完善的產業生態體系(ecosystem)，加速產業創新及優化產業結構，並充分利用我國既有優勢，進而掌握軟硬整合創新應用之契機，將是未來產業發展重點方向。

我國自2002年起推動國家資訊通信發展方案，至今逾10餘年，鑒於當前全球先進國家皆將數位經濟視為國家社會進步暨經濟轉型的主調，且政府目前推動產業創新及新南向政策，數位經濟為其重要驅動因素，「數位國家・創新經濟發展方案（2017-2025年）」（簡稱 DIGI+），除延續之前國家資通訊發展方案，並在硬體與軟體建設並重原則下，透過建構有利數位創新之基礎環境，鞏固數位國家基磐配套措施，打造優質數位國家創新生態，以擴大我國數位經濟規模，達成發展平等活躍的網路社會，推進高值創新經濟並建構富裕數位國家之願景。

本計畫將配合《數位通訊傳播法》及《電信管理法》修正草案，建構通傳業者國家資通訊安全防護機制，強化數位匯流及資訊安全，培育跨域數位人才，提供民眾安全可信賴應用環境，為數位國家・創新經濟發展方案「數位創新基礎環境」工作主軸之一。並與與刻正規劃之第五期國家資通安全發展方案緊密銜接，規劃以「打造安全可信賴的數位經濟時代」為願景，並以「建置國家資安機制，提升自我防護能量」、「培育資安專業人才，推動資安產業發展」、及「建立資安防護團隊，保衛數位國家安全」為目標，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」、「孕育優質資安菁英人才」4項策略，推動執行各項工作。

(二) 擬解決問題

大智移雲（大數據、智能化、移動網際網路和雲端運算）時代來臨，根據美國「戰略暨國際政策研究中心(Center for Strategic and International Studies, CSIS)」於2010年委託資安公司 Mcafee 之調查報告(In the Crossfire - Critical Infrastructure in the Age of Cyber War)指出，全世界各關鍵基礎設施多曾遭受各式威脅與攻擊。2010年起，伊朗核設施工業控制(Supervisory Control and Data Acquisition, SCADA)系統遭惡意不法組織以 Stuxnet 病毒攻擊，感染約三萬台以上電腦，導致伊朗納坦茲核設施的五分之一離心機被迫關閉，重創伊朗核子計畫。2011年 Stuxnet 之變種病毒 Duqu 蠕蟲出現，此惡意程式專門用於蒐集工業控制系統製造商之情資與擷取鍵盤敲擊在內之數位情報，以便未來對工業控制系統所控管之關鍵基礎設施發動攻擊。未來各國在關鍵資訊基礎建設所面臨的，將是更趨複雜且難以獨自處理的複合式威脅。

二、 計畫目標

因應每天數以萬計的資安事件及系統紀錄等需要被處理或管理，國內通傳事業(包含電信業者、IASP 業者、有線電視業者等)為了保護重要資源，均已建立各種資安防護系統來抵禦外部攻擊，常見設施包含：防火牆、防毒軟體、虛擬私人網路(VPN)、安全掃描相關系統以及入侵偵測系統(IDS)、入侵防禦系統(IPS)，網路應用程式防火牆(WAF)等，已廣泛運用在資安環境上。

本計畫預計整合資安技術與相關軟硬體建置，建立資安監控平臺 (C-SOC)，彙集多元資安情資來源，制定通傳事業資安通報應變機制(C-CERT)，提供資安事件分析、資安趨勢、資安關聯之資訊分析與分享(C-ISAC)，提升整體通傳事業資通安全水準，降低資安事件衍生之風險，保障國內資通安全與人民權益。

三、 計畫內容與實施策略

本計畫分項計畫名稱如下，執行策略說明如後:

分項計畫	細部計畫名稱
分項一　建構通訊傳播網路安全防護中心(CNSPC)	1.1 建置 CNSPC 備援機房 1.2 擴建網路運作管理平台(NOMC)新增通傳事業之網路障礙通報

分項二　建置 CIIP 新一代資訊分析與分享平臺(C-ISAC)	2.1 擴建 C-ISAC 新增通傳事業之雙向自動介接或網頁通報 2.2 擴建 IASP 佈點主機之威脅漏洞模擬功能
分項三 建置國際物聯網資安驗證實驗室	3.1 取得國際驗證單位 ul 授權及進行國際驗證單位 ul 實驗室之人才培訓 3.2 建置符合國際物聯網資安驗證規範(ul2900)之檢測實驗室

四、 實施範圍

本計畫實施範圍說明如下

(一)分項計畫一：建構通訊傳播網路安全防護中心(CNSPC)

1.1建置 CNSPC 備援機房

建置通訊傳播網路資通安全防護中心(CPSPC)備援機房，為提供業者最佳服務保障並確保系統持續正常運作。108年度預計於財團法人電信技術中心(路竹區)或國家通訊傳播委員會(南區監理處)擇合適位置進行備援機房之場域建置並規劃備援機房人員人力配置

1.2擴建網路運作管理平台(NOMC)新增通傳事業之網路障礙通報

108年將針對 NOMC 展示通報系統功能進行展示內容與功能之擴充及業者障礙通報平台欄位之擴增，俾達系統容量可滿足108年80%業者之收容與介接，並預計於109年滿足100%業者納管。

配合系統容量擴建，108年預計完成行動通信(4家含擴增1家)、固定通信(3家含擴增1家)、衛星通信(3家含擴增1家)及有線電視(52家含擴增17家)之網路運作通報暨核心架構圖資呈現系統，用以進行各業者的重要告警匯集、交付及解析，即時提供六大網路關鍵基礎設施運作狀態，並預計於109年100%完成。

(二)分項計畫二：建置 CIIP 新一代資安資訊分析與分享平臺 (C-ISAC)

2.1 擴建 C-ISAC 新增通傳事業之雙向自動介接或網頁通報

本子項工作於107年已完成12家網際網路服務業者成為 C-ISAC 運作機制之會員及雙向情資分享之模式。藉由資安監控分析通報平臺經訊息蒐集與彙整及分析之資安訊息，透過系統化方式即時分享，同時導入會員管理機制與運作架構，垂直與水平訊息交換機制與通傳適用 STIX 格式之建立，達成通傳事業資安聯防之目標，提升整體通傳事業資安防護之能力。

108年將進行系統容量擴建，預計完成24家通傳事業雙向資安訊息自動介接或網頁通報，109年預計累計達30家。

2.2 擴建 IASP 佈點主機之威脅漏洞模擬功能

本子項工作將持續監控特定漏洞成長情況，提供國家決策高層數據支援。今年度將建構至少擁有監控20個漏洞之能量，並視情況發展提供立即有效之防護對策建議或技術支援。為避免資源之虛擲，本項工作亦會建立漏洞監控資源需求之管理機制，刪除已無必要監控之漏洞。

(三)分項計畫三：建置國際物聯網資安驗證實驗室

《UL 網路安全保障計畫》(Cybersecurity Assurance Program, CAP) 應運而生，其根據美國聯邦政府、學術界與產業界重要利害關係人所提供的建議而制定，旨在強化關鍵基礎建設 (Critical Infrastructure) 中供應鏈的安全措施。該計畫援用全新 UL 2900 系列標準，能為連網產品與系統提供網路安全測試準則，以評估軟體漏洞與弱點、降低被入侵的風險、處置已知的惡意軟體、檢視保全控制項目，並提升大眾安全意識。目前 UL CAP 的服務與軟體安全作業已被美國國家資安行動計畫視為測試與認證 IoT 連網裝置的重要方法，特別是能源、公共 事業與醫療照護等重要基礎建設

3.1 取得國際驗證單位 ul 授權，進行國際驗證單位 ul 實驗室之人才培訓

「關鍵基礎建設的可用性與完整性跟社會安全與福祉息息相關。UL CAP 提供可靠的第三方認證支援，以及可評估連網產品與系統安全性與廠商流 程的功能，讓廠商以安全性為核心，開發與維護產品與系統。本子項工作將委由 UL，協助本實驗室取 UL2900實驗室授權及完成教育訓練，以提供國內廠商 UL2900

檢測服務，協助公私營機構的製造商、採購人員與終端使用者降低產品資安風險，進軍國際市場。

3.2 建置符合國際物聯網資安驗證規範(ul2900)之檢測實驗室

UL CAP 可幫助各界找出產品與系統中的安全風險，並提供降低風險的建議，包括工控系統、醫療設備、汽車、暖通空調製冷設備、照明產品、智慧家庭、家電、警報系統、火警系統、建築自動化、智慧電表、網路設備與消費性電子等產業；所採納的 UL 2900 系列標準不僅提供基本的技術條件，衡量並提升產品與系統的安全性，甚至能配合市場發展所產生的安全需求，適時建立與整合其他技術準則。在這其中，UL 2900 標準所涵蓋的組織評測 (Organizational Assessment) 還能協助評估供應商、系統整合商、資產所有人進行無疑慮之安全(Security) 產品與系統的設計、開發及維護等流程。

只要符合 UL 2900 系列標準所定義的條件，該產品或系統就能獲 UL 認定為「符合 UL 2900 標準」而取得證書與詳細測試報告。UL 已經成為美國國家標準 ANSI 及被 FDA 認可，UL2900可轉換提供 IEC 及未來其他認證需求。本子項工作係依據 UL 實驗室建議之檢測設備清單完成實驗室建置，達成相同之檢測技術水準，共同針對物聯網產品之設備弱點評估與攻擊檢測。

五、 計畫期程：108年1月1日至109年12月31日。

六、 關鍵績效指標及年度目標值

目標	預期成果效益	績效指標	評估方法	目標依據
分項一建構通訊傳播網路安全防護中心(CNSPC)	■建構通訊傳播關鍵資訊基礎設施之資安聯防機制，參與國家級跨域資安聯防體系，共同守護數位國家	■S2.科研設施建置及服務：CNSPC備援系統建置 1式(108年) ■Y.資訊平台與資料庫:完成行網(4家含擴增1家)及固網(3家含擴增1家)、衛星(3家含擴增1家)、有線電視 SO(52家含擴增17家)之圖資系統及網路運作告警系統 1式(108年)	依建置完成之實體平臺及通傳業者介	依前瞻基礎建設-數位建設4.1.4強化

	■掌握網際網路接取服務之資安事件及垃圾郵件情資，並建立與國內及國際相關組織之分享資安情資機制。	■Y.資訊平台與資料庫:完成100%通傳業者之圖資系統及網路運作告警系統 1式(109年)	接數進行評估	國家資安基礎建設計畫執行計畫
分項二 建置 CIIP 新一代資訊分析與分享平臺(C-ISAC)		■S2.科研設施建置及服務：完成24家(含新增12家)通傳事業參與 C-ISAC 平臺雙向資安訊息自動介接或人工分享(108年) ■S2.科研設施建置及服務：完成30家通傳事業參與 C-ISAC 平臺雙向資安訊息自動介接或人工分享(109年) ■S2.科研設施建置及服務：佈點主機之威脅漏洞模擬功能 1式(108年)		
分項三 建置國際物聯網資安驗證實驗室	■輔導國內廠商通過符合 UL2900 資安檢測規範之 IoT 產品,提升國內廠商國際市場競爭力	■S2.科研設施建置及服務：完成國際驗證單位 UL 實驗授權 ■S2.科研設施建置及服務：提供至少2家廠商取得 UL2900證照及完成測試報告		

七、 持續營運評估

在安全信賴的智慧臺灣,所有關鍵基礎建設所賴以維運的資通訊系統如電信與資訊網路系統、交通運輸管制系統、輸配電網路與電力調度系統、金融系統、健保與醫療系統、氣象監控與預測系統等關鍵資訊基礎建設,均需建構具備防禦縱深之資安防護措施。通傳會的資通安全防護中心及資通安全分析管理平臺為政府資安聯防重要角色之一,蒐集彙整通傳網路之網路運作狀況、網路障礙事件、災防事故及資安事件,進行相關事件分析及分享之智庫功能,計畫期程結束後,將以自有人力進行平臺後續維運,並編列公務預算支應後續平臺維運所需之經費。國際物聯網 資安驗證實驗室,則將培育自我檢測能量團隊,協助國內廠商

的產品就近取得測試及驗證服務，提高產品競爭力，並依 UL2900實驗室營運規劃，以技術服務費用爭取持續營運。

八、 經費明細概算

本計畫共執行四年，106年~109年分年 mile stone 及 endpoint 如下，另因應108~109年工作執行所需之經費明細概算如下。

年度 Mile stone	106年度	107年度	108年度	109年
建構通訊傳播網路安全防護中心(CNSPC)	■ 規劃通訊傳播網路安全防護中心(CNSPC) ■ NOMC:建立通訊傳播資通安全防護中心DNS網域及國際海纜之監控系統及其功能驗證	■ 完成通訊傳播網路安全防護中心(CNSPC)機房及系統建設 ■ NOMC:完成行動通信(3家)、固定通信(2家)、衛星通信(2家)、有線電視(35家SO)、國際海纜(8家含擴增5家)及DNS網域(10家含擴增5家)之圖資系統及網路運作告警系統	■ NOMC:完成行網(4家含擴增1家)及固網(3家含擴增1家)、衛星(3家含擴增1家)、有線電視SO(52家含擴增17家)	■ NOMC:完成100%通傳業者之圖資系統及網路運作告警系統 ■ 強化防護中心運作所需之加值服務系統功能
建置CIIP新一代資訊分析與分享平臺	■ CII ISAC:規劃新一代資	■ CII ISAC:蒐集國內外資安情資進行歸納、彙整	■ CII ISAC:完成24家(含新增12家)通傳事業與C-	■ CII ISAC:完成30家(含新增6家)通傳事業與C-

(C-ISAC)	安訊息交換平臺	與分析，完成通傳事業資安情資交換與分享 ■ 輔導通傳事業提供網際網路業者加入資安監控平臺(C-SOC)之資安事件與垃圾郵件佈點主機放置	ISAC平臺雙向資安訊息自動介接或網頁通報	ISAC平臺雙向資安訊息自動介接或人工通報 ■ 完成CII ISAC資安情資分享分析並達成以下指標:分享資安情資至IASP業者，每年至少15,000筆、分享資安情資至N-ISAC，每年至少6,000筆、移案垃圾郵件至IASP業者，每年至少30,000封、與合作國交換垃圾郵件，每年至少80,000封、經由TWCERT/CC與非合作國交換垃圾郵件，每年至少300,000封

分項三 建置國際物聯網資安驗證實驗室			■ 與 UL2900 確認及簽署合作契約 ■ 進行檢測儀器評估與採購 ■ 檢測人員教育訓練	■ 取得 UL 實驗室授權 ■ 提供國內物聯網設備廠商檢測服務
最終 end-point	■ 建構通訊傳播關鍵資訊基礎設施之資安聯防機制，參與國家級跨域資安聯防體系，共同守護數位國家 ■ 掌握網際網路接取服務之資安事件及垃圾郵件情資，並建立與國內及國際相關組織之分享資安情資機制。 ■ 輔導國內廠商通過符合 UL2900資安檢測規範之 IoT 產品，提升國內廠商國際市場競爭力			

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
				經常門	資本門		
108	1	分項一　建構通訊傳播網路安全防護中心(CNSPC)		4,794	25,000	同六、關鍵績效指標及年度目標值	1
	2	分項二　建置 CIIP 新一代資訊分析與分享平臺(C-ISAC)		8,305	7,500		1
	3	建置國際物聯網資安驗證實驗室		12,251	9,150		1
合　　計				67,000			

年度	項次	工作項目	工作內容	所需經費		績效目標	優先次序
				經常門	資本門		
109	1	分項一　建構通訊傳播網路安全防護中心(CNSPC)		4,003	10,000	同六、關鍵績效指標及年度目標值	1
	2	分項二　建置 CIIP 新一代資訊分析與分享平臺(C-ISAC)		6,044	7,500		1
	3	建置國際物聯網資安驗證實驗室		17,453	15,000		1
合　　計				60,000			

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
108Q2	30%	20,100	- 完成 CNSPC 備援機房、NOMC 擴充案、C-ISAC 擴充案採購規格澄清及進行採購程序 - 完成佈點主機新增功能開發需求書
108Q3	60%	40,200	- 完成設備採購作業程序，設備到貨安裝及測試中 - 進行系統建置與客製化需求開發 - 完成 UL2900確認及簽署合作契約

108Q4	100%	67,000	- 完成驗收、整合性試運行及驗收 - 繳交技術報告 - 依績效指標完成業者數目介接

時程	累計預定進度(%)	累計預定支用費用(千元)	關鍵查核點
109Q2	30%	6,300	- NOMC 擴充案、C-ISAC 擴充案採購規格澄清及進行採購程序
109Q3	60%	12,600	- 完成設備採購作業程序，設備到貨安裝及測試中 - 進行系統建置與客製化需求開發 - 取得 UL 實驗室授權
109Q4	100%	21,000	- 完成驗收、整合性試運行及驗收 - 提供國內物聯網設備廠商檢測服務 - 依績效指標完成業者數目介接與業者輔導

十、 預期效益

本計畫分項計畫目標一係透過通盤檢視目前通傳事業關鍵基礎設施資通安全防護現況，制定通傳事業關鍵基礎設施資通安全防護準則，件並監控通傳事業關鍵基礎設施資通安全防護運作及建立相關通報系統，以系統性提昇國內通傳事業關鍵基礎設施資通安全防護能力，強化通訊傳播關鍵基礎設施之網路防護能力，提升業者通報、應變及處置能力。分項計畫二則藉由研析先進國家通傳事業於資安監控與通報機制、垃圾郵件防制作法，分析我國實務執行面之差異，同時與通傳事業業者溝通、邀請其加入資安監控分析通報平臺及情資分享計畫，並將完成建立資安監控平臺 及資訊分析與分享平臺 ，可對於一般或特殊事件進行資安威脅、情資分析，並縱向、橫向與相關機關或通傳事業分享資安情資，亦將建立垃圾郵件分析中心及監控平臺，以提昇通傳事業整體對於垃圾郵件之防制及資安威脅情報綜整，俾能協助主管機關掌握網際網路接取服務之資安事件及垃圾郵件情資，建立與國內及國際相關組織之資安情資分享機制。

計畫最終預期效益為強化通訊傳播關鍵資訊基礎設施之資安防護能力，提升業者通報、應變及處置能力，建構通訊傳播關鍵資訊基礎設施之資安聯防機制，參與國家級跨域資安聯防體系，共同守護數位國家。

十一、 相關聯絡資料

國家通訊傳播委員會，吳政昇，3343-8232，kevinw@ncc.gov.tw