前瞻基礎建設計畫－數位建設

5G 資安防護系統開發計畫

（核定本）

經濟部

109 年 9 月

政府科技發展中程個案計畫書

審議編號：110-1401-09-20-04

經濟部技術處

「5G 資安防護系統開發計畫」

(核定本)

計畫全程期限：110 年 01 月至 113 年 12 月

目 錄

壹、基本資料及概述表(A003)

<table>
<tr><td>審議編號</td><td colspan="4">110-1401-09-20-04</td></tr>
<tr><td>計畫名稱</td><td colspan="4">5G 資安防護系統開發計畫</td></tr>
<tr><td>申請機關</td><td colspan="4">經濟部技術處</td></tr>
<tr><td>預定執行機關
(單位或機構)</td><td colspan="4">經濟部技術處</td></tr>
<tr><td rowspan="3">預定
計畫主持人</td><td>姓名</td><td>何祥瑋</td><td>職稱</td><td>科長</td></tr>
<tr><td>服務機關</td><td colspan="3">經濟部技術處</td></tr>
<tr><td>電話</td><td>02-23946000#2581</td><td>電子郵件</td><td>hwho@moea.gov.tw</td></tr>
<tr><td>計畫摘要</td><td colspan="4">依據總統宣示：「發展六大核心重點產業，以結合5G時代、數位轉型及國家安全的資安產業」之政策目標，符合5G基礎公共建設之「5G及物聯網資安防護」政策，針對5G系統資安5個面向進行研發：
1.5G安全所面臨之國際市場資安合規要求
2.網路功能軟體化衍生的資安威脅
3.通訊設備之供應鏈透明度不足
4.自有品牌市場機會浮現
5.隱私與個資保護需求與日遽增
故本計畫發展 5G 資安偵防系統，確保業者設置的5G系統是安全、可靠、可信賴的，並與國內 5G 專網業主合作進行服務驗證，建立在地 5G 專網資安解決方案實際案例，協助開拓國際市場。全程重點工作如下：

1.建構5G合規檢測技術：參考國際資安組織（如網路層3GPP/ITU、營運GSMA/ETSI/CSA）及歐美先進國家(美國NIST及歐盟ENISA等) 相關標準，並符合我國NCC資通安全維護計畫17項要求及系統審驗技術規範，除驗證公網之連線安全，更透過本計畫研發直領域資安合規（如HIPPA、IEC62443），並切入掃描虛擬環境弱點等面向，使5G專網符合各領域規範，以提升附加價值。本計畫所產出之工具將爭取納入國際或國內實驗室認可清單。
2.打造5G系統OSS資安事件偵測機制與防護指引：蒐集多樣態滲透攻擊實證 (包含網路層/虛擬層/網路功能等的攻擊案例),以完備公網的資安偵測規則，並進一步建構垂直領域專網FCAPS防護指引。監控管理5G網路</td></tr>
</table>

	虛擬化服務效能，完善應用層級資安隔離管理，提升5G垂直應用資安偵防技術水準，強化國產5G系統整體資安防護能力。 3.建立在地5G專網資安解決方案與場域合規性：加值國產5G設備與資安產業，打入國際供應鏈。將廣邀資安業者參與5G資安演練場域試驗，研發我國 5G資安自主技術，聯合資安廠商與5G業者共同攻擊測試場域，驗證資安合規性，提升5G應用廠商之競爭力。		
計畫目標、預期關鍵成果及其與部會科技施政目標之關聯	計畫目標	預期關鍵成果	與部會科技施政目標之關聯
	O1. 完成 5G 專網合規檢測技術，建立我國自主第三方檢測能力	O1KR1. 110 年完成 gNB、MEC(UPF、虛擬層)3GPP SCAS 檢測技術，111 年建立檢測實驗室測試作業規範，113 年取得 TAF 實驗室資格	經濟部:O1:強化產業創新研發價值
		O1KR2. 110 年完成 container 環境弱點管理工具，111 年與 112 年完成智慧製造、醫療照護領域法規合規工具，113 年取得驗證單位認可	
	O2. 建立 5G 安全滲透測試機制，打造 5G 的資安防護系統	O2KR1. 開發 5G 系統資安滲透測試工具，110 年建立公網及專網 40 個測試腳本以上，111 年累計 90 個以上，全程 4 年達 200 個以上，涵蓋 NIST SP 800-53 的 10 類安全控制	經濟部:O1:強化產業創新研發價值
		O2KR2. 建構 5G OSS 系統資安事件的偵測規則 110 年產出 20 條，111 年累計產出 50 條以上，全程 4 年達 100 條(以上)，以及專網資安威脅圖像（Landscape）與資安防護指引	
		O2KR3. 建立主動式 5G NFVI 網路效能監控機制，110 年完整支援虛擬機、及容器 2 類服務架構，111 年完成跨核網及邊緣平台整合，全程 4 年達可偵測 3 種類(連線、頻寬及延遲)應用層級服務異常，	

		生成對應資安防護規則	
	O3. 促進資安業者參與5G 應用場域實驗，建立在地 5G 專網資安解決方案實際應用典範	O3KR1. 110 年產出 5G 資安解決方案 3 項以上，111 年累計 5 項以上，全程 4 年達 10 項以上	經濟部:O1:強化產業創新研發價值
		O3KR2. 110 年強化國產 5G 產品之資安防護能力、協助台廠進入國際大廠可信賴供應鏈廠商 3 家，至 111 年累計 10 家	
		O3KR3. 110 年參與 3 個 5G 應用實驗場域進行 5G 資安解決方案實證，111 年累計參與 5 個以上，全程 4 年累計參與累計 8 個以上	
預期效益	全程目標與最終效益： 目標一：完成5G專網合規檢測技術，發展合規檢測工具，並完成實驗室測試作業規範，建立我國自主檢測能量。 目標二：建立5G專網資安評估機制，發展資安滲透測試工具、腳本與防護指引，強化5G專網的資安防護系統。 目標三：廣邀資安業者與相關協會參與5G資安場域，形成5G專網資安解決方案，豎立我國5G資安應用典範。 預期達成產業效益： 1.促進廠商產品資安合規，提高自主品牌的附加價值，打入國際市場 2.提升 5G 垂直應用資安水準，達成 5G 系統安全、可靠、可信賴的安全系統，加速 5G 整體產業發展		
計畫群組及比重	□ 生命科技 ____ %　□環境科技 ____ %　■數位科技 _100_ % □ 工程科技 ____ %　□人文社會 ____ %　□科技創新 ____ %		
計畫類別	■ 前瞻基礎建設計畫		
前瞻項目	□ 綠能建設　■ 數位建設　□ 人才培育促進就業之建設		
推動 5G 發展	■ 是　□ 否		
資通訊建設計畫	□ 是　■ 否		
政策依據	1.FIDP-20170201040000：前瞻基礎建設計畫：1.4 強化國家資安基礎建設 2.SRB-20180300000000：行政院2018年產業科技策略會議-5G應用與產業創新策略會議(臺灣5G行動計畫2019-2022年)：3.完備5G技術核心及資安方案		

<table>
<tr><td></td><td colspan="5">能量3.AI-20180401000000：台灣AI行動計畫：4.1提供實證場域，並建立高資安防護及親善介面之資料開放與介接平台。
4.CSIDAP-20180401000000：資安產業發展行動計畫 ：1.研析全球資安市場需求趨勢
5.STWB-01080102020000：科技發展策略藍圖 108-111 年：2. 強化國際交流，完善資安環境</td></tr>
<tr><td>計畫額度</td><td colspan="5">■ 前瞻基礎建設額度
110 年度 90,000 千元
111 年度 90,000 千元</td></tr>
<tr><td>執行期間</td><td colspan="5">110 年 01 月 01 日 至 111 年 12 月 31 日</td></tr>
<tr><td>全程期間</td><td colspan="5">110 年 01 月 01 日 至 113 年 12 月 31 日</td></tr>
<tr><td rowspan="2">前一年度預算</td><td>年度</td><td colspan="4">經費(千元)</td></tr>
<tr><td>109</td><td colspan="4">85,000</td></tr>
<tr><td rowspan="15">資源投入</td><td>年度</td><td colspan="4">經費(千元)</td></tr>
<tr><td>110</td><td colspan="4">90,000</td></tr>
<tr><td>111</td><td colspan="4">90,000</td></tr>
<tr><td>112</td><td colspan="4">90,000</td></tr>
<tr><td>113</td><td colspan="4">90,000</td></tr>
<tr><td>合計</td><td colspan="4">360,000</td></tr>
<tr><td rowspan="5">110 年度</td><td>人事費</td><td>40,500</td><td>土地建築</td><td>0</td></tr>
<tr><td>材料費</td><td>732</td><td>儀器設備</td><td>0</td></tr>
<tr><td>其他經常支出</td><td>48,768</td><td>其他資本支出</td><td>0</td></tr>
<tr><td>經常門小計</td><td>90,000</td><td>資本門小計</td><td>0</td></tr>
<tr><td colspan="2">經費小計(千元)</td><td colspan="2">90,000</td></tr>
<tr><td rowspan="5">111 年度</td><td>人事費</td><td>40,500</td><td>土地建築</td><td>0</td></tr>
<tr><td>材料費</td><td>732</td><td>儀器設備</td><td>0</td></tr>
<tr><td>其他經常支出</td><td>48,768</td><td>其他資本支出</td><td>0</td></tr>
<tr><td>經常門小計</td><td>90,000</td><td>資本門小計</td><td>0</td></tr>
<tr><td colspan="2">經費小計(千元)</td><td colspan="2">90,000</td></tr>
<tr><td>中程施政計畫關鍵策略目標</td><td colspan="5">推動產業創新研發</td></tr>
</table>

<table>
<tr><td>本計畫在機關施政項目之定位及功能</td><td>1.依據總統宣示：「發展六大核心重點產業，以結合 5G 時代、數位轉型及國家安全的資安產業」，符合 5G 基礎公共建設之「5G 及物聯網資安防護」政策，並參考行政院「5G 應用與產業創新策略 (SRB) 會議」、「數位國家・創新經濟發展方案」與「台灣 5G 行動計畫」政策目標，在我國自主之 5G 行動通訊系統產品技術基礎上，建立自主資安防護能力，共同發展 5G 創新應用。本計畫聚焦建構 5G 系統之資安防護與產出網通產品之資通安全合規檢測技術。
2.計畫願景：建構國內 5G 專網進行服務驗證技術，打造在地 5G 專網資安解決方案實際案例，確保國產 5G 系統之資通安全是安全、可靠、可信賴。
3.計畫定位及功能：初期因應 5G 專網設備出口合規需求，研發 5G 安全標準檢測技術，提出實驗室測試作業規範，取得認可實驗室資格，建立我國自主檢測能力；研發 5G 資安防護系統，強化公網的偵測規則，建立完備的專網防護指引；上述研發成果，透過技術轉移及與相關公協會合作，促成網通設備業者、電信營運商和資安業者等，參與 5G 應用資安演練場域實驗，介接處內　5G 計畫（5G+系統暨應用淬鍊計畫）之專網實驗場域，進行資安防禦驗證。全程協助產業研發 5G 資安技術，打造 5G 資安防護機制，推動 5G 資安產業發展，強化國產 5G 產品之資安防護能力。</td></tr>
<tr><td>計畫架構說明</td><td>依細部計畫說明
<table>
<tr><td>細部計畫名稱</td><td colspan="5">5G 資安防護系統開發計畫</td></tr>
<tr><td>110 年度
概估經費(千元)</td><td>90,000</td><td rowspan="2">計畫性質</td><td rowspan="2">產業應用技術開發</td><td rowspan="2">預定執行機構</td><td rowspan="2">經濟部技術處</td></tr>
<tr><td>111 年度
概估經費(千元)</td><td>90,000</td></tr>
<tr><td>細部計畫
重點描述</td><td colspan="5">初期因應 5G 專網設備出口合規需求，研發 5G 安全標準檢測技術，提出實驗室測試作業規範，取得認可實驗室資格，建立我國自主檢測能力；研發 5G 資安防護系統，強化公網的偵測規則，建立完備的專網防護指引；上述研發成果，透過技術轉移及與相關公協會合作，促成網通設備業者、電信營運商和資安業者等，參與 5G 應用資安演練場域實驗，介接處內 5G 計畫（5G+系統暨應用淬鍊計畫）之專網實驗場域，進行資安防禦驗證。全程協助產業研發 5G 資安技術，打造 5G 資安防護機制，推動 5G 資安產業發展，強化國產 5G 產品之資安防護能力。</td></tr>
<tr><td>主要績效指標
KPI</td><td colspan="5">110年KPI：
1. 產出5G資安解決方案3項以上
2. 強化國產5G產品之資安防護能力、協助台廠進入國際大廠可信賴供應鏈3家以上。
3. 完成5G垂直應用場域進行資安解決方案實證3個以上</td></tr>
</table></td></tr>
</table>

		111年KPI： 1. 產出5G資安解決方案累計5項以上 2. 強化國產5G產品之資安防護能力、協助台廠進入國際大廠可信賴供應鏈累計達10家以上。 3. 完成5G垂直應用場域進行資安解決方案實證累計5個以上
前一年計畫或相關之前期程計畫名稱	109-1401-03-21-02：5G+系統暨應用淬鍊計畫(1/4)	
前期計畫或計畫整併說明	109-1401-03-21-02：5G+系統暨應用淬鍊計畫(1/4)之分項二	
近三年主要績效	執行5G資安偵防系統研發計畫： 1.依據3GPP SCAS研發檢測技術，完成研發基站檢測技術，並測試國產小基站產品，發現數個安全議題，進而與基站廠商持續就5G SA產品合作檢測技術研發。透過將資安檢測導入網通設備生產流程當中，從產品面提升整體安全之工具技術，以資安加值我國優勢產業。 2.完成開發5G垂直應用場域之資安偵防系統雛形，針對阻斷服務攻擊（DDoS）之偵測與減緩技術。透過建構SDN私有雲防護架構，進行惡意流量辨識、私有雲封包標記及減緩對應措施，進行惡意流量辨識與私有雲封包標記及減緩對應措施，且不影響5G低延遲特性。 3.完成研發 Container-based DDoS 攻擊工具，可彈性有效率產生 DDoS 檢測能力，涵蓋 11 種 DoS 工具整合至 5G 專網核心模組。完成對 TTC 商業及 III 企業專網之 5G EPC 核網做滲透測試作業，涵蓋 5G 核網元件(如 EPC、MME、S-GW 及 P- GW)與通訊協議(如 S1-MME/S1-AP、GTP-C、GTP-U)，進行滲透測試、DDoS 攻擊與弱點實證，以提升訊令協定弱點檢測能力。 4.接軌歐盟 H2020 之 ANASTACIA 專案，介接該計畫之 Security Orchestration 平台，完成開發安全策略轉譯模組，並建立整合界面結合 Open Source MANO（VM 環境）與 Kubernetes（Container 環境）。另結合工研院資通所 X 組的 Kubernetes 虛擬化平台技術，協助廠商自主建立系統解決方案之技術能力。	
跨部會署計畫	□ 是 ■ 否	
中英文關鍵詞	資訊安全, 安全保障規範, 5G 資安偵防系統, 資安合規, 資安檢測 Cyber Security, Security Assurance Specification, 5G Cyber Security Dectection and Defense System, Security Compliance, Security Testing	

計畫連絡人	姓名	張智翔	職稱	研究員

	服務機關	經濟部技術處		
	電話	02-23946000#2583	電子郵件	chchang5@moea.gov.tw

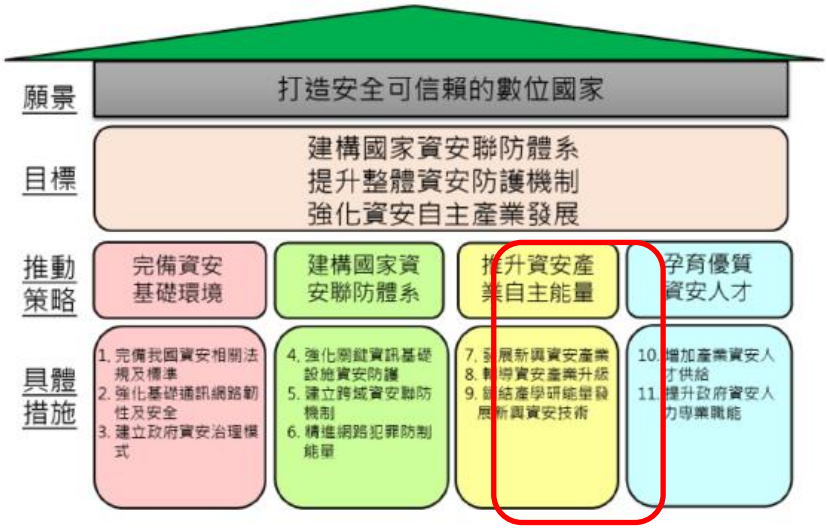
貳、計畫緣起

一、政策依據

1. 本計畫依據 107 年 10 月 31 日「5G 應用與產業創新策略（SRB）會議」決議，5G 時代來臨資安威脅更甚以往，針對 5G 科專技術成果及國內網通產品，應布局自主創新 5G 資安解決方案，發展 5G 資安偵防系統，並與國內 5G 專網業主合作進行服務驗證，建立在地 5G 專網資安解決方案實際案例，加值科專技術成果及國內網通產品，提升我國 5G 產品競爭力，協助開拓國際市場，並強化臺灣自主資安防禦能量。期達成資安防護形塑臺灣 5G 品牌，及「5G 產業資安化」、「5G 資安產業化」之目標，以建立完整的 5G 通訊資安產業鏈。

2. 政府於產業發展方面，提出「五+二產業創新計畫」之「國防（資安）」產業為策略性推動重點，強化資安技術自主研發能力，推升本土資安產業在技術研發與能量的精進，確保國家安全、社會安全和個人安全，作為我國發展數位經濟的堅實後盾，落實「資安即國安」之政策目標。

3. 行政院資通安全處提出「國家資通安全發展方案（106-109 年）」，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，達成「打造安全可信賴的數位國家」願景，擬定四項推動策略：完備資安基礎環境、建立國家資安聯防體系、推升資安產業自主能量與育孕優質資安人才。



資料來源：「國家資通安全發展方案（106至109年）」（106/11）

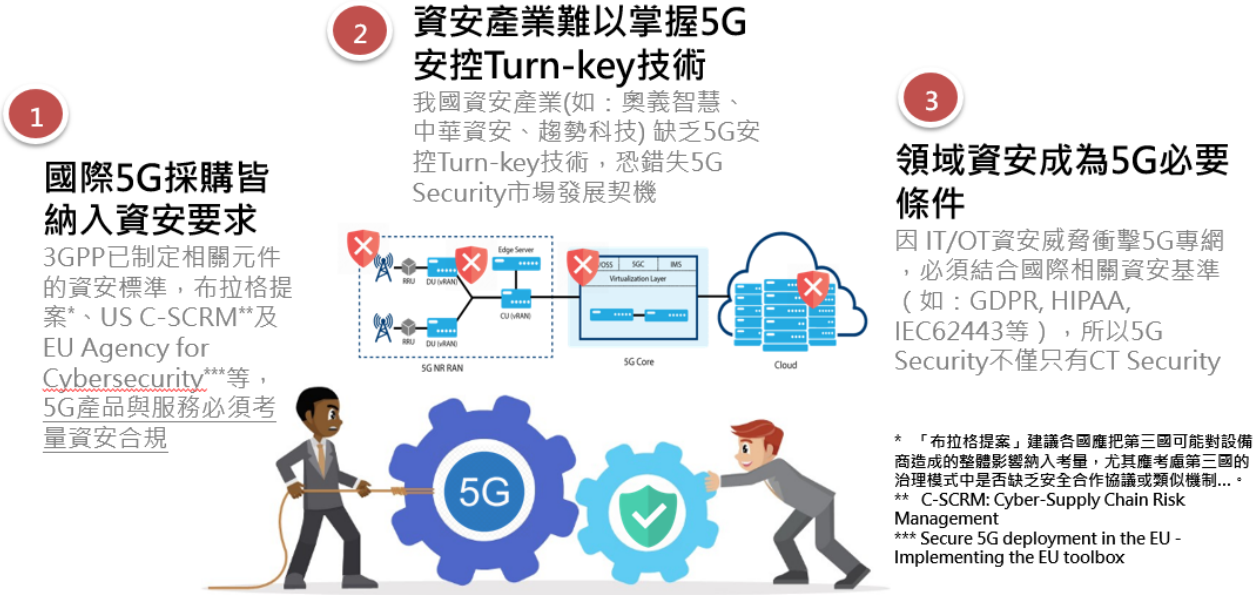
圖 1：國家資通安全發展方案發展藍圖

4. 依據行政院「數位國家、創新經濟發展方案」，本計畫於奠定「數位基磐」在我國自主之 5G 行動通訊系統產品技術基礎上，須儘快建立自主資安防護能力，共同發展 5G 創新應用。

5. 依據 108 年 6 月行政院核定之「台灣 5G 行動計畫」完備 5G 核心及資安防護能量推動主軸，針對 5G 科專技術成果及國內網通產品，發展 5G 網路資安之偵防系統，並積極協助國內網通業者落實 5G 產品合規檢測，加速國產 5G 產品進入市場之目標。

二、擬解決問題之釐清

資通安全與隱私保護為 5G 系統發展的必要需求，然開放架構與軟體定義的 5G 特性，使 5G 系統暴露在資安威脅中，故產業對資安技術需求迫切。本計畫針對 5G 系統元件與軟體化/虛擬化環境的資通安全需求進行盤點：(1)由於國際上逐步對 5G 系統採購納入資安要求，但是國內網通設備廠商（如小基站、MEC 製造廠商）尚未具有資通安全確保的能力，可能因資安沒有合規而喪失訂單，所以網通廠商與資安服務業者急需填補 5G 資安合規檢測技術；(2)資安產業尚未掌握通訊協定資安威脅來源，與管理層面 OSS（Operations support system）資料深度分析技術對 5G 資安的關鍵性，以及針對專網應用情境整合 IT、OT、CT 的資安解決方案，將錯失 5G 資安防護市場契機。



資料來源：本計畫自行整理

圖 2：5G 資安技術缺口

資料來源：本計畫自行整理

圖 3：國內 5G 資安需求盤點

1. 各國法規要求/5G 虛擬化/SDN 網路、國內 5G 合規檢測產業缺口

(1) 國內缺乏 5G 資通安全檢測能量：國際業主與電信商逐步要求國產網通產品通過第三方檢測，但國外檢測價格昂貴，國內 5G 通訊檢測能量不足，本土資安服務商難以提供協助。

(2) 資安產業尚無 5G 應用合規驗證工具：5G 垂直應用在各領域皆有安全標準要求，如智慧製造(IEC62443)、醫療(HIPAA)，維運時亦需保證持續合規，導致設備進入門檻極高，且個資隱私法規(GDPR)日益嚴格，但國內資安服務對各標準合規技術明顯不足，形成技術缺口。

2. 專網維運防護需求缺口、困境

(1) 5G 專網中大量採用 x86 架構、虛擬化元件、軟體定義網路、網路功能虛擬化，藉此提供更加敏捷與多元化的服務，並減少硬體維護上產生的人力需求，使得開放原始碼軟體的需求大增，也讓 5G 專網維運的資安問題隨之而來，現今常見企業級的資安事件，除經由社交工程的誘捕，更為主動的攻擊為目標環境中有其中極小元件安全設置，讓攻擊者加以利用致使擴散至整個環境。此外，由於開源專案的貢獻者為不特定對象透過網路同步進行審核，原始碼撰寫風格的不同會增加維運方面的成本，且貢獻者可能無意或刻意在貢獻的程式碼中暗藏漏洞，如 Linux 系統曾發生有貢獻者嘗試貢獻有漏洞的原始碼。5G 專網的相關應用，如智慧城市、能源等關鍵基礎設施，如遭受資安威脅，將可能造成大規模毀滅性災害，如交通號誌錯亂、全區電力大斷電。

(2) 5G 在面對不同垂直應用場域時，所產生的資安問題漸趨複雜，傳統的資安事件基本發生於單一的設備上，而在 5G 垂直場域不僅針對每個場域不同微調，其中最大的不同為每個應用場域都有可能是不同的設備，同時

有可能採取不同的應用層與傳輸層規範，造成網路傳輸資訊時的不一致性，而防護也沒有一個完全通用的方案，如流量同步需求、加解密規範以及資安防護嚴密程度。現有資安業者雖有卓越的資安人才，然而，難以即時根據不同場域偵測與防護專網資安威脅。

3. 核網管理層面的技術缺口

(1) 5G 專網須建構自主資安協作平台：由於 5G 應用主要透過虛擬化佈署，將帶動虛擬層管控平台迅速發展。市面上尚未有主導性的產品，系統整合商須使用不同的 OAM (operations, administration and maintenance)管理 5G 虛擬化系統環境，廠商將面臨整合維護上的困難，而且維運廠商必須提高操作人員的知識背景，以補足技術與維運能力缺口。

(2) 5G 開源平台內嵌資安機制研發：5G 專網與相關應用目前仍以功能與效能為主要開發導向，資安問題相對尚未受到重視，隨著 5G 核網支援的網路功能增加，搭配虛擬層的相關應用後的資安維運將相對複雜，整體會更難以控管內部資安政策（Security Policy）。

4. 5G 網路虛擬化環境追蹤惡意攻擊來源之技術缺口

(1) 5G 應用大量使用虛擬化元件完成 NFV 服務。虛擬化平台 (Kubernetes）的執行環境，方便於正常程序執行，然惡意攻擊常隱藏於正常連線，如缺乏追蹤連線的機制會導致惡意攻擊無法追蹤。保護正常程序與服務運作是重大課題，如何快速追蹤網路連線，快速隔離，是 5G 應用上的重要問題。

(2) 5G 專網的目標之一是提供自主性給 5G 專網擁有者，然而 5G 專網擁有者缺乏資安實務經驗，無法對網內設備依據需求快速設計和調整符合領域應用所需的資安防護策略和措施。

(3) 容器(container)消失時資料也隨之逝去特性，讓 5G 業者、系統整合業者和資安業者等，難以立即解決 5G 專網受到不當設定問題，或遭受 API 伺服器不當存取的資安事件，及難以在事後透過取證方式還原事發現場。

三、目前環境需求分析與未來環境預測說明

1. 5G 資安自動化檢測技術研發

(1) 國產設備外銷資安需求

A. 目前環境需求分析 ：在 5G 之前，相關通訊設備為大廠把持，而 5G 時代小基站需求興起，且設備功能朝虛擬化與分層雲端化方向發展，我國自有品牌設備(如小基站、Security Gateway、MEC 產品)有了切入的市場機會。然而，國內資安檢測能量僅限於 IT 領域，對於通訊

技術相當陌生，難以滿足國產設備進入國際市場時的資安檢測需求。

B. 未來環境預測：國際上對資安要求日益強烈，且 3GPP SCAS（3rd Generation Partnership Project, Securit Assurance Specification）安全確保標準也逐步制定更嚴格的測試要求，GSMA（Global System for Mobile Communications）的通訊安全認驗證機制也從試營運階段進入正式階段，在標準制定與認驗證機制成熟的推動下，5G 網通設備將被要求更高的資安水準，才具備進入國際市場資格。

(2) 專網合規需求

1. 目前環境需求分析：5G 網通設備連結物聯網形成整合性應用，而各垂直應用領域皆有其資安標準，且 5G 網路建設也必須滿足合規需求。部分應用領域(如醫療 HIPAA)的 5G 專網建置到已推動合規多年，具備高成熟度的應用場域，將面臨達到與原環境相同合規程度的挑戰。另外新興應用領域，如智慧製造資訊安全或隱私保護的合規需求，資安標準仍持續制定或剛推出未久，5G 專網面對的是如何因應應用特性的合規挑戰。

2. 未來環境預測：由於各應用領域智慧化發展程度越來越高，隨著 5G 專網市場將蓬勃發展，使得應用服務架構越趨複雜，若要持續性的保持合規狀態，意味著不僅是定期稽核，更須自動化的合規管理與風險評估機制，將為 5G 專網的合規技術帶來更大的挑戰。

2. 5G 安控與主動式防禦技術

(1) 資安威脅偵防技術

A. 目前環境需求分析：智慧工廠使用 5G 專網提升產能、醫療院所藉由專網導入創新醫療模式，建置專網的需求提高。雖然系統整合廠商能為業主建置專網，但其缺乏專網資安維運經驗，如果專網系統遭受入侵突然斷線，無法達成網路傳輸穩定、及時與資安強韌，不僅將造成停止運作、營運損失，甚至嚴重影響生命安全。故需建構 5G 資安自主資安維運技術，並技轉系統整合廠商或資安服務廠商

B. 未來環境預測：由於專網的自主性、客製化、隱密性，帶來生活與生產的便利性，所以預期未來不同產業皆有機會導入 5G 專網。為保持專網資安維運需要 7/24 的投入，不同的產業因其背景知識的差異，在佈署上需有不同維運策略，須以自動化機制提升資安維運轉成效

(2) 5G 開源平台內嵌資安機制研發

A. 目前環境需求分析：5G 專網擁有者需能解讀系統內防禦措施的數

據和事件；若無法解讀和關聯來自網元日誌內容意義及建立運行基準線，將無法有效判斷攻擊事件與威脅來源。當運行時遭遇疑似資安議題或是應用場域需求改變時，若無維運中日常運行樣態和資源使用量基準線，5G 業者、系統整合業者和資安業者難以在有限情報下，在短期內規劃適切的資安防護措施和調整策略。

B. 未來環境預測：面對資安攻擊手法不斷進化及領域應用需求和目標不斷調整的情況，5G 專網需要配備能夠綜觀全局且具自動化和智能化的偵測、分析和關聯動態行為能力的資安偵蒐系統，因此在 OAM (Operations, Administration, and Maintenance) 層面上迫切需要自動化和智慧化的監控系統與安全性資訊與事件管理解決方案，讓 5G 業者、系統整合業者、資安業者和 5G 專網擁有者能夠因應不斷變動的外在環境，打造領域應用所需的整體資安防護策略和措施。

(3) 網路功能虛擬化系統資安研發

(1) 目前環境需求分析：5G 核心網路會使用到 NFV，而 NFV 又以佈署在虛擬化環境為主。在各種虛擬化技術中，以容器 (Container) 因為輕量化的特點最被看好，因此容器 環境的資安研究，在現在與將來都是重要的環節。各廠商對於虛擬化環境的資安保護多針對單一節點，而 NFV 在運作上又以結合多節點的方式提供服務。因此整合多節點的通訊，並繪製成軌跡 （Communication trajectory） 在 5G 核心網路上，成為一個必要卻又缺乏的技術。

(2) 未來環境預測：面對將來 5G 核心網路使用 NFV，逐漸以多節點整合方式提供服務，開發綜合多節點的安全服務將成為重要的技術。本研究所提供的技術，預期讓 5G 業者、系統業者與資安業者面臨頻繁變動的環境，能更有效率的保護系統安全、改善系統效能，進而提供更有品質的服務。

3. 5G 創新資安服務場域實證

(1) 專網資安威脅塑模

A. 目前環境需求分析：從世界現況來看現行 5G 商用系統都是採用 NSA（Non-stand alone）架構，也就是將 5G 技術做為補充頻段，這種技術被稱為固定無線接入(Fixed Wireless Access, FWA)，目的是取代 WiFi 或固網光纖等接取技術，利用 5G 的高頻寬提升連網速度與整體吞吐量，免除電信業者與專網場域佈線之苦，但是在這種用例中，並未充分發揮 5G 系統的開放性與軟體化能力，無法原生提供 uRLLC（Ultra Reliable Low Latency Communications）與 mMTC（Massive

Machine Type Communications）服務。為了實現 5G 致能的願景，當 5G 專網系統演進至 SA 架構，雲端技術(如 MEC, Multi-Access Edge Computing)與營運支援系統(OSS)必然需要被引入至專網環境中，如何營運這些系統是專網業者過去未曾擁有的能力，另一方面如何整合 5G SA 系統與既有系統與應用服務(Legacy Systems and Services)是另一個 5G 專網系統的挑戰，為了向下相容這些老舊系統，勢必將既有威脅引入 5G 專網中。這些非屬連線安全議題，故並不是 3GPP 標準處理的議題。

(1) 未來環境預測：5G 專網依照主管機關通傳會（NCC）之規劃，專網頻段處於 4.8G-4.9GHz，目前尚需等待內政部移頻，預估需到 2021 年才能移頻完成，再開放企業申請營運驗證（POB），故目前 5G 專網從概念驗證（POC）到 POB 預估還有兩年的等待期。而 POC 與 POB 之重大差異在於對於資訊安全要求的納入，POC 僅需證明 5G 功能需求正常，但 POB 需符合各方期待，故 5G 專網的 POB 階段須要考量以下四個面相向：(a) 領域主管機關(如經濟部、交通部或衛福部)與 NCC 的通訊監理要求;(b) 國內外的資安標準(如 IEC 62443、HIPAA 或 GDPR)；(c) 日新月異的 5G 新興威脅與與時俱進的 5G 資安圖像(Threat Landscape)；(d) 保證 5G 專網本身服務水準，除了通訊層安全外，5G 專網還包含計算平台層，應用系統層與資料層都需要依照內部需求與外部威脅來規劃其安全架構（Security Architecture），確保 5G 專網系統的可用、可靠與強韌。

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

1. 社會經濟

為提供國人與企業安全、可靠、可信賴 5G 垂直應用發展環境，本計畫針對 5G 系統「事前預防」研發網通產品資安檢測技術，與「事中偵測」開發專網主動式安全防護機制，確保 5G 系統在事前能保證設備之資通安全，於事中可不斷透過偵測機制保護網路安全，強化 5G 重要關鍵應用（如智慧娛樂、智慧醫療、智慧工廠）在自主資安技術的保護下蓬勃發展，並提升國產網通設備之資安防護力，打入國際市場。

2. 產業技術

透過接軌國際通訊安全標準 3GPP SCAS，以及參考相關施做指引，建構 5G 元件與軟體化環境之資安檢測工具。同時，橋接歐盟 H2020 之 ANASTACIA 計畫，引入資安策略管理技術於 5G 防護系統，提升關鍵防護技術的自主率；

研發之 CT 資安成果將串聯業界成熟之 IT 資安防護技術，與資安業者發展專網資安解決方案，共同建立創新資安服務模式。

3. 生活品質

鑑於 5G 資安已是國際上強烈關注議題，各國政府相繼提出法規，強化電信與專網廠商對 5G 系統的安全要求，以提供國民一個安全的 5G 使用環境。本計畫產出之技術可增進 5G 系統資安防護力，協助電信廠商通過主管機關的資通安全審查，並提升國內專網安全性，降低專網系統遭受惡意攻擊、外部入侵與隱私資料外泄的風險，提供更安全、穩定的 5G 生活服務（如智慧醫療、智慧娛樂）品質。

4. 環境永續

由於 5G 的開放架構與軟體化特性，將帶來更廣泛的威脅面向，為因應 5G 網路新型態攻擊，必須與時俱進強化維運期間的資安監控能力。本計畫發展具持續更新的安控技術與主動式防護機制，並結合資安廠商成熟的 IT 資安防護技術，以及連結其他相關使用者設備的檢測技術（如物聯網計畫）能量，提供 5G 網路 E2E（End to End）的永續資安維護環境。

5. 學術研究

5G 專網在關鍵的 uRLLC（Ultra-Reliable Low-Latency Communication ）應用（如智慧醫療、智慧製造）上，須考慮資安防護機制可能帶來的延遲，而造成整體效能的 QoS（Qaulity of Service）無法達標，以至造成生命財產的重大損失。可透過學術之前瞻研究，針對低延遲應用提供高效率的資安偵防機制，確保 5G 需要 uRLLC 特性的服務，達成安全、可靠與高可用性的目標。

6. 人才培育

5G 資安為新興通訊領域的資安議題，本計畫將積極推動培育 5G/B5G 技術之頂尖資安研發/檢測人才及 5G 跨域應用資安威脅盤點人才，供未來產、學、研發展使用。也將透過 5G 資安鑄造及創新資安服務模式之合作方式，連結網通廠商、系統整合廠商、電信營運商、資安服務業者等，引導台灣 CT、OT、IT 人才與產、學、研單位、彼此交流、共創合作，累積 5G 應用之資安實務經驗人才。

7. 促進性別平等：

(1) 本計畫屬研究類計畫，研發計畫內容以推動產業創新研發為目的，其專業團隊係以資通訊領域畢業生為主，目前國內女性畢業生僅占 3 成，致整體相關領域人才仍以男性居多，將續持鼓勵更多理工背景之女性人員參與，加強培育及延攬與 5G 資安相關專業領域之女性研究人才，提升女性專業技術研發能力。

(2) 如有規劃辦理活動，將注意性別均衡性，亦將統計參加者人數及回饋意見之性別統計與性別分析，作為未來精進之參考。

(3) 本計畫目前參與人員除規劃團隊持續推動少數性別參與計畫外，未來如與廠商合作或配合經濟部辦理活動時，將鼓勵女性人員參與，希望藉由更多女性人員參與，促進兩性比例平衡，消除職業性別隔離，亦將進行性別統計分析，並蒐集回饋意見，以作為後續辦理活動之參考依據。

參、計畫目標與執行方法

一、目標說明

鑒於各國 5G 基礎建設之採購皆陸續納入資安要求，5G 垂直應用的資安成為 5G 發展的必要條件，然資安產業尚無法掌握 5G 安控統包解決方案（Turnkey）技術，故本計畫研發目標：(1) 打造 5G 專網合規檢測技術，研發資通安全檢測工具，提升 5G 產品之資安等級；(2) 建立 5G 安控與主動化防禦技術，強化 5G 專網的資安防護系統；(3) 發展 5G 資安鑄造及創新資安服務模式，朝向服務導向資安情資服務發展。產出成果將協助網通廠商、系統整合業者與資安服務產業掌握 5G 資安全球商機，且提升 5G 相關產業之資安能量，發展 5G 資安鑄造及創新資安的服務模式。

1. 5G 資安自動化檢測技術研發

計畫全程總目標				
發檢測技術與自動化設定與弱點管理工具，使 5G 專網符合垂直應用資安標準要求，進而在維運階段都能持續合規，且綜整風險資訊以制定資安修補策略				
年度	第一年 民 110 年	第二年 民 111 年	第三年 民 112 年	第四年 民 113 年
年度目標	智慧製造法遵合規技術與基站測試規範制定	智慧醫療法遵合規技術與 5G 檢測實驗室成立	隱私法遵合規技術與合規工具認可	5G 維運合規設定檢測技術與專網協作整合
預期關鍵成果	•調適 SCAS 測試個案基準，發展智慧製造領域安全標準 (IEC62443-4) 之合規檢測技術，並完成 TAICS 基站測試規範制定。 • 研發 IEC62443-4 標準之組態管理與風險評估工具，自動化定期檢測，提供稽核證據。	•發展智慧醫療領域標準 HIPAA 與 HITECH 合規檢測技術，並成立 TAF 5G 檢測實驗室。 •研發應用領域規範切換機制，並確保 API 介面安全，以協助 5G 專網產品適用各種應用場域。	•建立隱私稽核法規檢測技術，使 5G 專網符合 GDPR，合規相關工具申請國內驗證單位認可。 •開發資料控管保護技術，比對檔案、存取差異，偵測開源套件竄改等功能，輔助隱私稽核佐證。	•整合 5G 系統、環境、維運等階段之組態檢測技術，提供整體風險評估資訊，訂定資安修補策略。 •透過 5G 核心管理機制，分析並檢測動態協商參數之合規性，並與資安協作機制整合，即時修補高風險議題。

2. 5G 安控與主動式防禦技術

(1) 安控項目查驗技術與資安威脅偵防技術

計畫全程總目標
發展安控項目檢驗技術，將驗證概念實體化，確保通訊網路可符合營運基本安全

守則。研發通訊網路威脅偵防平台，連結資安情資系統，進行低延遲封包分析符合 5G 網路提供高速網路特性。				
年度	第一年 民 110 年	第二年 民 111 年	第三年 民 112 年	第四年 民 113 年
年度目標	安控項目查驗工具包-權限控管及身分驗證與防護智慧工廠多接取邊緣運算安全	安控項目查驗工具包-不可否認性及資料機密制定 5G 資安應用安全規範，強化資安防護系統。	安控項目查驗工具包- 通訊安全及資料完整性與完成 5G 專網偵防平臺，進行 5G 與傳統防禦平臺整合	安控項目查驗工具包- 可用性及隱私與完成建構 5G 專網資安關連系統。
預期關鍵成果	完成兩類安控項目查驗工具包，可檢驗權限控管及身分驗證類別，並於通訊網路場域實用 研發多接取邊緣運算主動防禦機制，建立權限控管機制，並進行小規模誘捕介接大規模獵捕	完成兩類安控項目查驗工具包，可檢驗不可否認性及資料機密類別，並於通訊網路場域實用 訂定 5G 專網資安施作指引，提供場域端於專網營運時的資安施作策略與方法，並研發專網自動化滲透測試模組，以判斷專網資安強韌性	完成兩類安控項目查驗工具包，可檢驗通訊安全及資料完整性類別 ，並於通訊網路場域實用 藉由 5G 信令攻擊手法及核網效能監控指標，研發核網異常防禦機制，結合傳統資安防禦機制成為專網資安威脅偵搜平臺	完成兩類安控項目查驗工具包，可檢驗可用性及隱私類別，並於通訊網路場域實用 結合行為監控、惡意行為偵測、惡意行為攔阻技術，並透過分析偵測結果，來關聯出攻擊來源與根因，進而達到自動化事件關聯

(2) 5G 內嵌資安整合協作平台

計畫全程總目標				
發展內嵌資安整合協作平台，於虛擬化平台上建立自動防護反應機制。透過開發不同的 Policy interpreter 以擴大支援更多的虛擬化平台，以符合 5G 大規模物聯網之特性，同時確保環境符合 IEC 62443，提供營運商 5G 完整解決方案。				
年度	第一年 民 110 年	第二年 民 111 年	第三年 民 112 年	第四年 民 113 年
年度目標	資安協作平台功能完善性提升	強化協作平台對資安設備之涵蓋率與支援度	強化協作系統對其它虛擬化平台與資安機制之相容性	內嵌資安協作平台商業化
預期關鍵成果	強化 Orchestrator Policy 應用後仍保有相當品質的 QoS 服務，開發	強化 Policy Interpreter 與 Security Enabler，使 orchestration 可以針對不同	支援其它不同如 k3s 或 VMware 等的 Virtualization layer 來開發支	以商業導向為主軸，依據前期成果與廠商回饋來為內嵌資安協作平台進行收斂性

	redundancy conflict 與 priorities conflict 等兩種以上的衝突檢測與修正機制要件，讓內嵌防護協作平台具備商業產品之穩定度	Layer 的 network policy 做描述與轉譯，提高內嵌防護平台之產品價值與通用性	援 5G VNF 的 Security Enabler 與 interpreter，持續改善協作平台之支援度與完善性	質的開發及維護，整合相關資安業者產出，提供 5G 資安服務協作解決方案

(3) 網路功能虛擬化系統資安研發

計畫全程總目標				
建立主動式 5G NFVI 網路效能監控機制，支援虛擬機、及容器服務架構，偵測連線、頻寬及延遲等應用層級服務異常，並生成對應資安防護規則。				
年度	第一年 民 110 年	第二年 民 111 年	第三年 民 112 年	第四年 民 113 年
年度目標	容器服務可視化	動態資安策略生成	資安策略動態佈署整合	專網服務資安融合管理
預期關鍵成果	可互動檢視容器服務程序 TCP/UDP 連線關係與延遲、消耗頻寬等網路品質參數之界面工具。	可主動學習服務常態服務品質規格，自動生成對應資安策略之管理工具。	可依實際服務品質需求，動態將資安及效能監控策略套用至專網 NFVI 資安管理模組，強化資安防護隔離。	結合 5G 資安檢測模組、日誌監控模組，建立完整資安防護模型，成為持續監控防護 5G 專網之資安強固機制

3. 5G 創新資安服務場域實證

(1) 專網資安威脅塑模

計畫全程總目標				
連結雲端安全、營運安全、資料安全與通訊安全之安全議題跨界整合，弭平新舊技術融合之落差，提出全面且持續之風險評估技術				
年度	第一年 民 110 年	第二年 民 111 年	第三年 民 112 年	第四年 民 113 年
年度目標	專網裝置身分辨識與存取管理	5G 基礎設施與既有系統威脅辨識與減緩	強化營運效率，保護專網個人資料與隱私安全	專網軟體與網路元件透明與可信
預期關鍵成果	以零信任策略進行裝置聯網存取權限之管控，提出 5G 專網連網裝置種類與身分辨識技術。	融合具安全評估功能之軟硬體元件，與既有系統隔離/過濾等營運安全策略，研製安全政策強化軟體功能	在避免侵害個資前提下，透過網路元件、應用服務之資料，提出持續性風險評估技術。	以軟體物料清單(SBOM)，評估專網軟體與網路元件透明度與可信度，整合於前一年度之持續性風險評估技術。

二、執行策略及方法

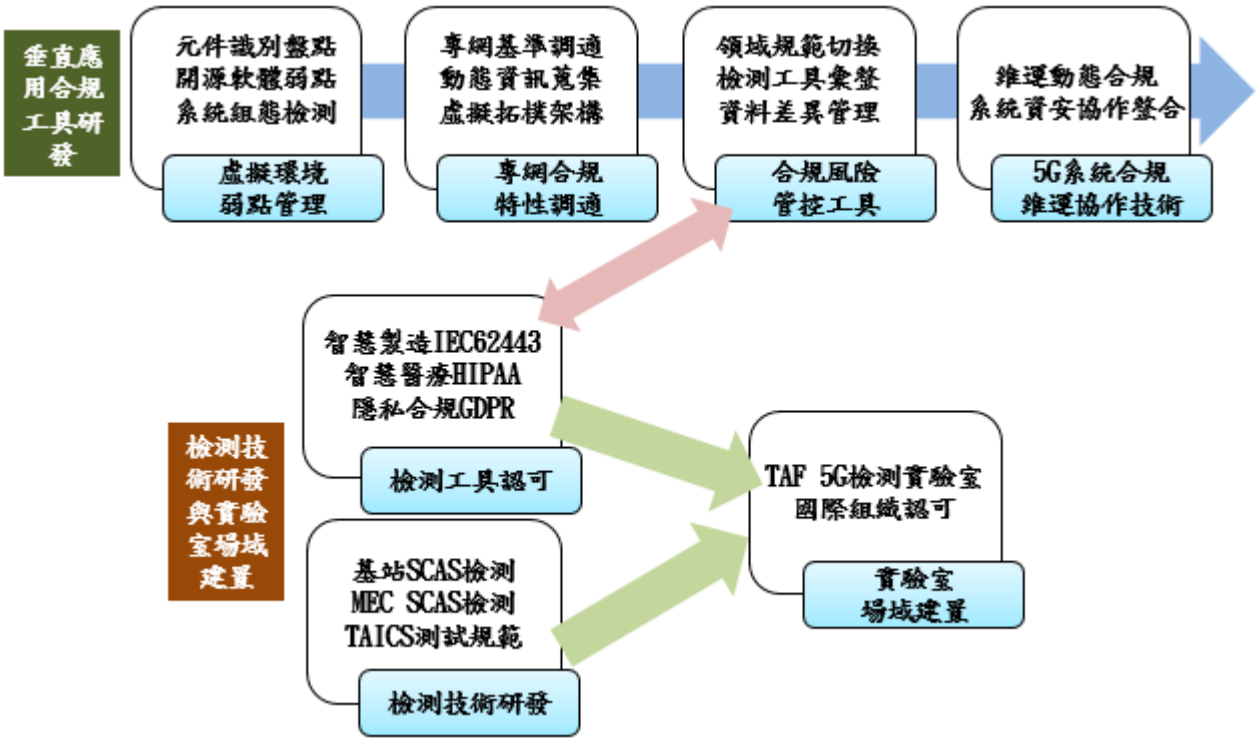
為確保 5G 系統元件與軟體化環境之資安防護能力，本計畫研發 5G 網通產品(如小基站、MEC 核網元件）資安檢測流程/測項，以及針對白牌虛擬化平臺安全，發展弱點檢測技術、應用領域合規檢測（如：醫療 HIPAA、工控 IEC62443）。研發成果將建立 5G 資安國際檢測合規能力，並透過台灣資通產業標準協會（TAICS）訂定 5G 小基站及 MEC 資安產業規範，促使國產 5G 元件符合國際資通安全標準。

因應專網系統維運期間的新形態攻擊威脅，本計畫打造基於 OSS（Operations Support System）深度資料分析能力的資安偵防核心技術，研發符合國際 5G 資安框架（如 NIST SP 800-53）之安控（Security Control）洞察力，以及開發主動式防護與內嵌資安整合協作（Security Orchestration）技術，建構威脅攻擊的防護網。

計畫成果將結合實驗場域(如臺中智機）與商用場域(如系統整合廠商、電信業者合作)，進行 5G 專網資安威脅建模與資安風險評估；並整合 5G 專網合規檢測技術與 5G 安控自動化防禦技術，與資安業者發展專網資安解決方案。

1. 5G 資安自動化檢測技術研發

本分項為 5G 資安合規技術研發，執行策略分為兩個層面，合規檢測技術研發與實驗室場域建置，如下圖所示。



資料來源：本計畫自行整理

圖 4：5G 資安合規技術研發之主軸規劃

為解決 5G 合規所面對的產品出口與垂直應用領域合規議題，需研發適用於 5G 設備環境的檢測技術與自動化合規工具。由於合規檢測技術的研發成果需具備公信力，除需將成果推動國內產業標準制定，公開給設備商與實驗室做為功能研發或檢測依據外，亦需取得國內外驗證組織的認可。因此須進行實驗室場域建置，包括實驗室成立過程與工具取得認可之經驗，並可轉移強化國內第三方檢測能量。

2. 5G 安控與主動式防禦技術

(1) 安控項目查驗技術

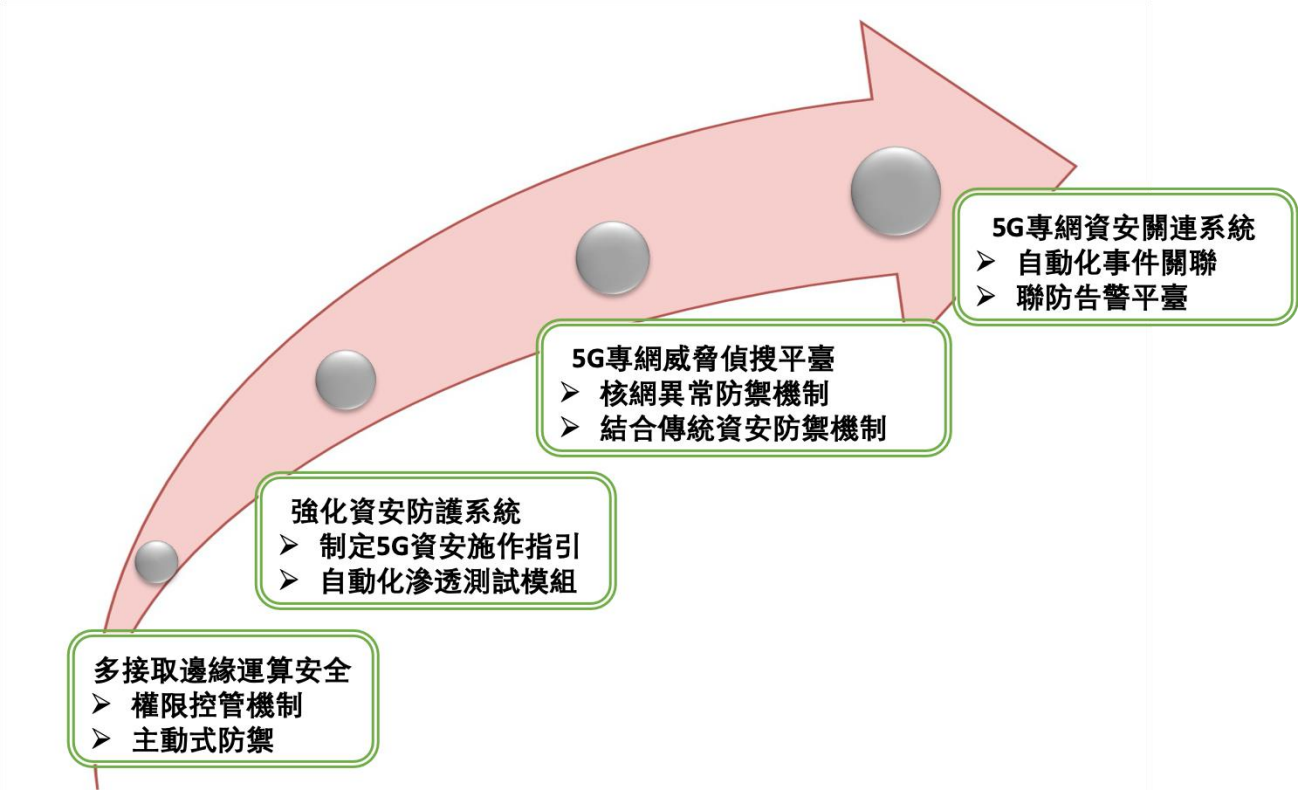
隨著行動寬頻網路持續演進，5G 的技術的網路由公眾網路延伸至企業專網，為維持專網的營運可用性，資訓安全需考量面相向比以往傳統網路更為迫切。專網安全的基礎架構便是確保網路運作，需符合通訊系統安全框架的規範。參考 ITU-T X.805 所提安全架構將安全維度分為八種，並對接美國 NIST SP800-53，開發營運安全控制項查驗工具包，依四年度規劃，第一年開發可檢驗權限控管及身分驗證類別工具，次年開發不可否認性及資料機密類別工具，第三年開發通訊安全及資料完整性類別工具，第四年開發可用性及隱私類別工具。結合與 NIST 合作 5G security 計畫，建立 5G 場域安控檢查機制 best practice

(2) 資安威脅偵防技術

為了建立 5G 專網安全評估機制，打造 5G 專網的資安防護系統，先以服務為主體的多接取邊運算作為切入點，進行應用服務權限控管，並透過主動式防禦機制誘捕入侵威脅，進行第一層保護。協同 5G 產業廠商，召開專網場域防護策略論壇，並訂定 5G 專網施作指引，提供專網維運參考，避免專網系統的維運漏洞產生。並利用自動化滲透測試模組，測試場域強韌性。

結合電信網路特有威脅及核網效能管理指標平台特徵，研發關連核網威脅防禦機制，期望布建於垂直應用場域中，由於核網可用性需要維持，核網下層的網路架構一但被攻陷便無法保持核網運作，故整合傳統資安防禦機制為專網資安威脅偵搜平臺。

設置 5G 場域攻防平臺，針對不同特性的設備，調校專用於該設備特徵之型態，藉由外部實際攻擊與惡意程式測試，主動發掘新興威脅手法與特徵，進而將資訊回饋至 5G 資安偵防平台，透過攻擊與防禦機制同時存在的平台，於 5G 虛擬容器環境，結合行為監控、惡意行為偵測、惡意行為攔阻技術，並透過分析偵測結果，來關聯出攻擊來源與根因，進而達到事件關聯分析。



資料來源：本計畫自行整理

圖 5：5G 新型態攻擊實證與防護技術進程

(2) 5G 內嵌資安整合協作平台

資料來源：本計畫自行整理

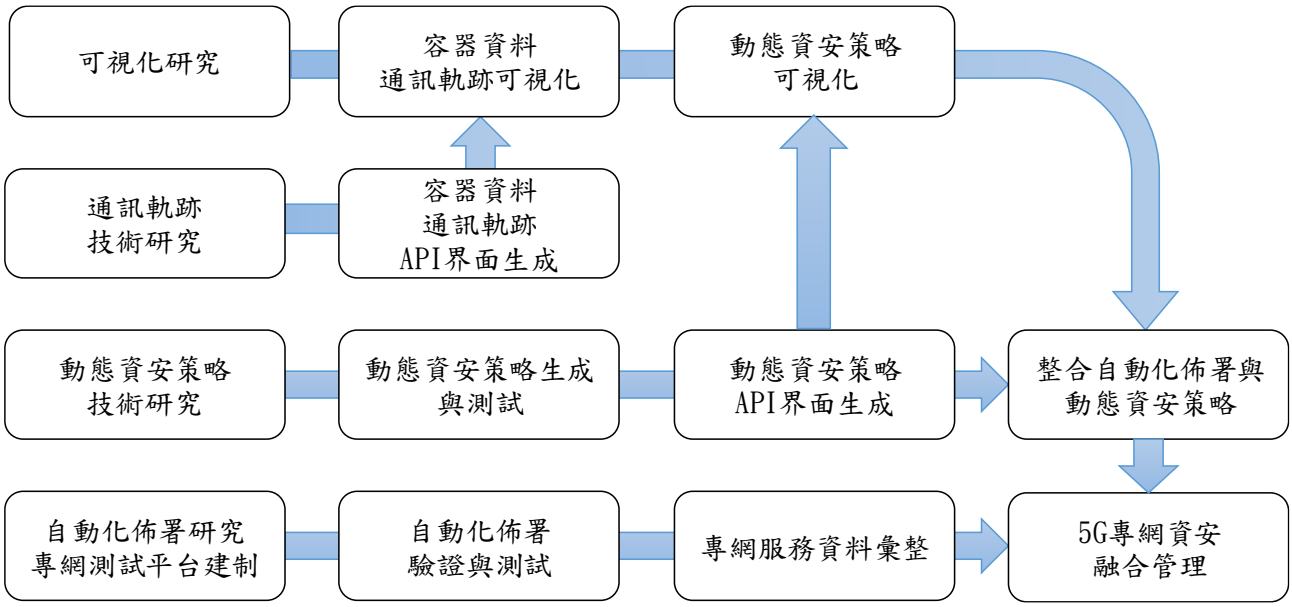
圖 6：5G 虛擬化內嵌資安平台開發與分析

於 109 年科發基金計畫之成果中，已完成內嵌防護協作平台的雛型規畫與關鍵元件串接，並導入至工研院虛擬化平台 kubernetes 上，與自主 5G 專網進行整合測試。FY110 團隊將強化 Orchestrator 的完整度，在 Interpreter 的部份開發支援 throughput、errorRate 等相關設定的從屬性質，確保 Policy 應用後仍保有相當品質的 QoS 服務。Orchestrator 部份則開發 redundancy conflict 與 priorities conflict 等兩種以上的衝突檢測與修正機制要件，提升 Security Orchestration 在資源分配與管理的完整性。

FY111 將著重強化 Policy Interpreter 與 Security Enabler，使 orchestration 可以針對不同 Layer 的 network policy 做描述與轉譯，從 L2/L3 延伸至 L7 (http、mail service)。開發 Security Orchestration Layer 4 - Layer 7 Access Control List 架構，並整合國內外支援 IEC 62443 Switch 進行測試，如研華 EKI 系列 、Cisco IE 系列、Moxa EDS 系列等等。分析資安策略並建立特徵值資料庫進行比對，以 IEC 62443 為最高原則，訂定資安策略衝突檢測與通報機制。FY112 則是針對其它不同如 k3s、vmware 等的 Virtualization layer 來開發支援 5G VNF 的 Security Enabler 與 interpreter，同時整合相關子項 API，包括 5G 外部偵防機制，5G 核網合規與註冊程序檢測機制等相關介面，提升協作平台完整度。FY113 開始以商業導向為主軸，依據前期成果與廠商回饋來為內嵌資安協作平台進行收斂性質的開發及維護。

(3)網路功能虛擬化系統資安研發

整合虛擬機為基礎的 APM 系統技術於 Kubernetes 平台；開發以容器為基礎的 APM 系統技術於既有之 NFVI 平台進行可行性評估與驗證。保護基於微服務的應用程序，開發微網段隔離 (Micro-Segmentation) 技術，提供 5G 應用程式與元件在 Kubernetes 環境擁有可靠的安全性配置與資安防護；並研究動態資安策略生成方法，提供自動化產生微網段隔離策略與佈署；最後讓開發完成之技術，與其他資安管理融合，提供完整的資安服務。



資料來源：本計畫自行整理

圖 7：網路功能虛擬化系統資安研發之主軸規劃

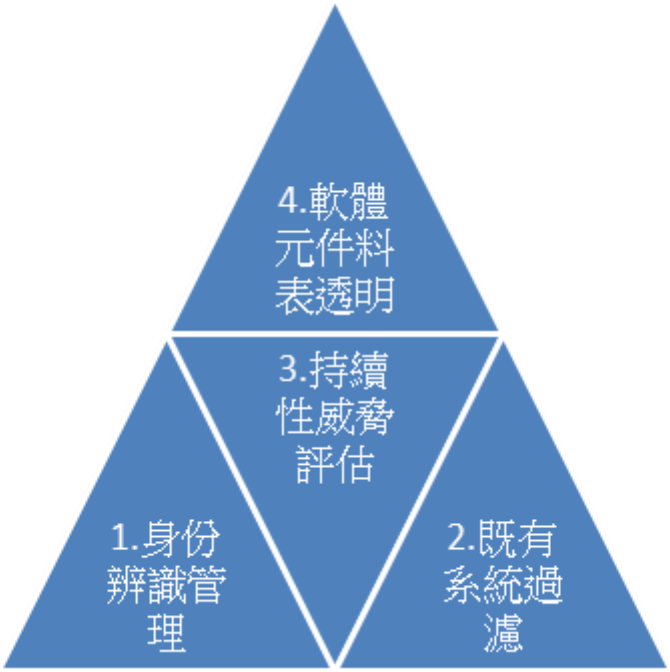
3. 5G 創新資安服務場域實證

專網資安威脅塑模

隨著 5G 技術商品化的持續成熟，許多民生相關服務必然選擇 5G 技術作為其通訊載體，採用 5G 專網作為其通訊基礎設施，其結果導致 5G 專網成為資安不法份子垂涎的目標。5G 專網採用了大量軟體化技術，使得原先 IT 世界的攻擊技術亦可於 5G 專網使用；5G 專網亦引入雲端計算技術，使得無論是電信業者或者專網設施擁有者被迫學習虛擬化部署與營運技術，這是新的挑戰，例如 2019 年 Cloudflare 因為軟體更新導致服務中斷。最後 5G 專網也需要處理與既有系統融合的問題，既有系統亦可造成固有威脅被引入 5G 專網。基於 5G 軟體化與可程式化的特色，過去一年一次的資安威脅評鑑的方法恐無法適應如此敏捷的開發交付需求，這需要開發適用 5G 專網資安威脅塑模技術，在此本計畫採用 Gartner 所提出之持續自適應風險與信任評估(Continuous Adaptive Risk and Trust Assessment，CARTA)，提出對 5G 應用領域具有上下文情境的感知能力，且能主動的在網路層與應用層收集 5G 專網的運作數據，強調在建立基礎架構時，就埋入安全架構要求，使整個安全管理時，具有完整的風險能見度，使用數據以評估現下風險，並排定資源投入的優先順序。

本分項為 5G 專網威脅評估技術的研發，有別於前一分項的偵測與監控技術所強調的事中分析，本分項強調是從事前就扣合外部要求與內部營運目標，降低威脅發生的可能性與衝擊性，執行策略分為四個層面，1.身分辨識與管控管理，2.既有系統(Legacy systems)的隔離與過濾，3.持續

性威脅評估，4.軟體元件料表(BOM)的透明度與可信任執行技術，如下圖所示。



三、達成目標之限制、執行時可能遭遇之困難、瓶頸與解決的方式或對策

1. 5G 資安自動化檢測技術研發

(1) 場域取得不易

A. 說明：研發成果需於垂直應用場域實證，但可能難以取得場域，或專網部署進度未如預期。

B. 對策：

(A) 與 5G 科專研發團隊合作，共同於場域實證。

(B) 透過 5G 合作廠商，藉由垂直應用合規檢測服務的執行進入場域，逐步達到實證的目標。

(2) 軟體工具需經過第三方認可

A. 說明：所研發之垂直應用合規檢測工具，為強化其公信力，期望取得垂直應用第三方檢測認可，確認可提供具備認證稽核效力之檢測結果。

B. 對策 :透過 TAICS 平台，與第三方檢測實驗室建立合作關係，深入瞭解合規稽核作業，並認可自動化檢測工具之效力。

2. 5G 安控與主動式防禦技術

(1) 5G 專網資安需要多重防護

A. 說明：5G 核網以 x86 架構運行電腦為基礎，已不再是過往特殊架構硬體，容易因為 IT 架構遭受駭客攻擊。

B. 對策：核網維運需要考慮到核網安全以及 IT 架構的安全性兩方面

(2) 缺乏實際專網場域：

A. 說明：5G 專網為新型態場域，甚至連完整的 SA 解決方案都未上市，難有實際運作場域可供實證。

B. 對策：由於資安所團隊正進行 5G 國產核網開發，可借此進入合作場域進行場。威脅驗證，也會利用資安所原有開發之核網與學界及業界建立前瞻服務探索的 5G 專網環境，作為多產業實證案例，建立防禦情資蒐集平臺，羅列 5G 資安威脅情資轉化為偵測手法。

(3) 商轉產品的演算法模型取得不易且複雜

A. 說明：FY110 著重在 network policy 的衝突與簡化，依照現成商轉產品的演算法模型來設計不僅取得不易，也較為複雜。

B. 對策：將目標放在學術論文與國際期刊，從中選擇適合的 policy 分析演算法，並搭配 5G 專網應用裡優先權較高的測試情境來開發。

(4) 應用場域數據取得不易

A. 說明：研發成果（解讀 5G 專網數據、5G 專網動態行為模型、異常動態行為剖析和偵測、異常行為取證）所需數據需來自垂直領域之應用場域的實況數據，但可能難以取得應用場域實際運行狀況和邏輯，或是專網佈署進度未如預期。

B. 對策：

a. 基於可取得領域之應用場域之樣本，再透過數據生成 (data generation) 或數據增強 (data augmentation) 方式創造更多合成數據，完成特徵捕捉和模型建立。

b. 與 5G 科專研發團隊合作，共同於應用場域進行實證。

c. 透過 5G 合作廠商，透過垂直領域之應用場域之資安檢測服務的執行進入場域，逐步調校、達到目標，以貼近真實性。

(5) 5G 創新資安服務場域實證

(1) 專網資安威脅塑模缺乏責任歸屬與共識

A. 說明 :專網為新興技術，與既有系統融合時，資安威脅塑模缺乏責任歸屬與共識。

B. 對策：

(A) 與 5G 科專研發團隊合作，共同於場域實證，提出可操作之經驗與可轉移之技術。

(B) 透過 5G 合作廠商，進入場域，逐步達到實證的目標。

四、與以前年度差異說明

1. 5G 資安自動化檢測技術研發

為使 5G 專網符合垂直應用資安標準，所研發之檢測技術與工具將逐年推進，從 110、111 年應用角度的智慧製造、製慧醫療，在 112 年則切入區域法規的隱私需求，可強化前兩年的垂直應用檢測技術，而在 113 年則研發系統部署與資安協作系統整合，以達到持續性合規的目標。

其間所產出的檢測工具，將申請標準認證，確保可適用於垂直應用合規檢測，並成立實驗室，藉由 TAF 認證，提升檢測流程與測項品質。

年度 差異項目	110 年度	111 年度	112 年度	113 年度
垂直應用合規工具研發	以 109 年開發的合規基準與工具為基礎，依據智慧製造安全標準調整基準值及增修功能。	從智慧製造進入智慧醫療，依法規調整基準與功能，並確保 API 介面安全。	著重於隱私標準合規的基準與功能增修，並開發資料異動偵測相關功能。	研發維運時期動態合規檢測功能，並與資安協作系統整合，即時修補高風險議題。
認證檢測工具		智慧製造檢測工具申請標準認證	智慧醫療檢測工具申請標準認證	
成立實驗室	109 年進行基站測試規範制定，於 110 年完	制定 MEC 測試規範，成立 TAF 5G 檢測實驗		

	成，並開始進行 TAF 5G 檢測實驗室申請。	室。		

2. 5G 安控與主動式防禦技術

(1) 安控項目查驗技術與資安威脅偵防技術

為使 5G 專網能查證網路是否有符合營運安全控制項，依四年度發展安控項目查驗工具包，確保網路符合安全規範。110 年以多邊緣運算為偵防標的，111 年、112 年以及 113 年則針對整個專網範圍進行全面性的考量，於 111 年提供自動化滲透工具，112 結合傳統網路防禦平台並於 113 年加入情資機制，提升偵防強度。

年度 / 差異項目	110 年度	111 年度	112 年度	113 年度
安控項目查驗技術	研發權限控管及身分驗證查驗工具	研發不可否認性及資料機密查驗工具	研發通訊安全及資料完整性查驗工具	研發可用性及隱私查驗工具
資安威脅偵防技術	進行應用服務權限控管，並透過主動式防禦機制誘捕入侵威脅	藉由真實場域補助訂定 5G 專網資安應用安全規範，提供施作指引及自動化測試模組，以判斷專網資安強韌性	整合傳統防禦平台至 5G 專網中，並完成 5G 專網資安威脅偵蒐平臺	關聯各種異質的防護設備告警訊息，用來關聯出攻擊來源與根因，進而達到自動化事件關聯

(2) 內嵌資安整合協作技術

年度 / 差異項目	110 年度	111 年度	112 年度	113 年度
資安整合協作平台	因應不同專網應用情境的資	針對跨網路層的網路政策加	於資安協作平臺上，擴大支	針對資安協作平臺的虛擬化

	安與隱私需求，可能在執行面出現重複或衝突的策略，故強化衝突資安政策檢查與修正機制，確保服務品質的 QoS	強連通性，增進 Security Enable 對不同網路層的支援性，提升資安管理平臺的有效性	援虛擬層（如輕量化與商業版本之虛擬層）提供具 VNF 的 Security Enalber 和 Interpreter	管理部分，增加 VMware、OpenStack 或 VirtualBox 等業界常用套件的支援性

(2) 網路功能虛擬化系統資安研發

本研究有預期開發容器服務監控機制，110 年度將相關數據可視化；111 年度依據彙整容器資料、通訊軌跡後，產生動態資安策略；112 年度因應頻繁變動的容器環境，開發自動化佈署機制；並開發自動化 API 介面，提供整合；最終於 113 年度整合 5G 專網資安管理。

年度 差異項目	110 年度	111 年度	112 年度	113 年度
容器服務可視化	可視化技術研究與實作	容器資料、通訊軌跡彙整	動態資安策略可視化	專網服務資料彙整
動態資安策略生成	可行性研究	動態資安策略生成與測試	動態資安策略 API 界面整合	整合自動化佈署與動態資安策略
資安策略動態佈署整合	自動化佈署技術研究	資安策略自動化佈署驗證與測試	資安策略自動化API界面整合	整合自動化佈署與動態資安策略
專網服務資安融合管理	專網服務平台建置	專網服務 API 界面整合與研究	專網服務與動態資安策略、自動化佈署、可視化界面整合研究	完成 5G 專網資安融合管理

五、跨部會署合作說明

本計畫不適用此節。

肆、近三年重要效益成果說明

1. **5G** 資安自動化檢測技術研發

   (1) 完成組態設定合規檢測工具 CSK，可匯入 NIST SCAP 格式之資安基準，檢測範圍涵蓋 Windows、Linux 等數千個檢測項目，技轉國內廠商等廠商。

   (2) 制定行動應用 APP 基本資安規範及測試基準，至 107 年 9 月推動國內第三方資安檢測實驗通過 TAF 認證達 10 家，依據測試基準研發 APP 自動化檢測工具，提供 APP 開發業者自動檢測功能，提升 APP 安全強度，保障消費者權益。制定影像監控系統 (IP CAM、DVR、NAS) 資安標準及測試規範，通過 TAICS 審查，推動國內第 1 家 IP CAM 資安檢測實驗室於 107 年 9 月通過 TAF 認證。

   (3) 制定智慧巴士車載資通訊系統 (智慧牌站、車載機) 資安標準及測試規範，通過 TAICS 審查。

2. 5G 新型態攻擊實證與防護

   (1) 完成智慧聯網韌體弱點分析技術雛形研發，可檢測 IoT 智慧設備 (如：IP CAM) 密碼暴露、金鑰與憑證暴露等多項資安問題，檢驗效率優於多款開源韌體安全分析程式 (如：FMK 與 Binwlk)。

   (2) 檢驗 5 款以上市面智慧聯網設備資安問題，成功發掘 2 款市面 IP CAM 產品潛藏資安後門漏洞問題，檢驗結果通報廠商協助修復。

   (3) 研發 Container-based DDoS 攻擊工具，可彈性有效率產生 DDoS 檢測能力，並且應用於核網場域檢測，並產生強化 5G 環境安全之效益

   (4) DDoS 衝擊減緩架構，利用 kernel 層過濾技術 XDP，來解析封包特徵值，降低網路延遲率。可彈性佈署於網路介面前端。進行惡意流量辨識、封包標記及減緩對應措施。

3. **5G** 開源軟體資安研發

   (1) SDN 與 4G/5G 軟體定義網路基礎建設：FY106 先進通訊實驗環境建置與技術研發計畫，運用 SDN 開源技術進行虛擬網路自動測試平台開發，並將開發結果與台灣網通設備商合作，部署至 2016 Computex Taipei 及 2017 世大運實證場域進行 SDN 測試。

   (2) OPNFV 與 4G/5G 虛擬化雲端開源平台：2017 年以 Openstack 原生雲為基礎，使用 Fuel Installer 進行 OPNFV Colorado 3.0 安裝與部署，並與日本

OOL 進行 Multi-site vRouter 使用情境開發，研究成果於 2017 年 OPNFV 北京高峰會進行發表。同年代表資策會申請加入國際 OPNFV 開源組織，並於台北舉辦第一場 OPNFV Meetup，進行國際網路開源技術交流。2018 年進行 OPNFV Fraser 6.0 研究，並採用具有遠端自動開關機之 IPMI 技術及結合 Apex Installer，完成實機與虛擬化環境之自動化部署及 Functest 測試。

(3) Orchestrator 與 4G/5G VNF 自動化開源部署技術：2017 年使用 Cloudify 進行 vRouter、vIMS 等 VNF 自動化部署；2018 年使用德國 Fraunhofer 所研發之 OpenBaton 自動化編排技術，進行 Iperf Client/Server 之 VNF 部署。

(4) FY107 年研發「企業內駭客橫向擴散偵測」，相關技術整合為「企業惡意橫向移動來源 IP 偵查技術」及「企業內橫向移動視覺化比對技術」，共計導入 2 項關鍵設施場域、1 項企業場域，完成技術實證或持續維運監控。同時發展惡意程式行為分析技術，發表 1 篇國際論文、3 案專利申請；研發「工控自動化防禦規則產生技術」技轉泓格科技公司，研發新一代工控網通資安防護設備，相關技術並於 107 年 8 月導入台水公司板新廠進行場域實測，淬鍊新產品效能。

(5) 整合情資萃取技術與企業內網潛伏威脅技術，FY107 與數聯資安公司合作「資安威脅情蒐平台」，運用於衛福部 ISAC 系統，提供醫療領域資安情資，並持續合作新北市區域聯防系統，整合資安情資蒐集到「企業潛伏威脅偵測平台」監控分析服務，以國內自主產品替代國外產品，落實行政院打造國家級資安聯防機制。

4. 網路功能虛擬化系統資安研發

免代理式應用效能管理系統(AAPM)結合 OpenStack KVM 虛擬機管理功能，入圍 2018 年全球百大科技研發獎(R&D 100 Awards)。

伍、預期效益及效益評估方式規劃

本計畫為達成建立我國 5G 技術自主能力，加值科專技術成果及國內網通產品，並帶動有資安防護能力之 5G 產品供應廠商，進入國際供應鏈，期達成資安防護形塑臺灣 5G 品牌，及「5G 產業資安化」、「5G 資安產業化」之目標，以建立完整的 5G 通訊資安產業鏈。全程預期效益分述如下：

1. 5G 產業資安化

(1) 依據 3GPP 安全確保要求所發展之落實度驗證技術，可於 5G 產品出廠或導入環境前，驗證其安全協定落實度，可防範惡意或無意間產生之後門，除可強化我國網通業者對資安重視程度，提升產品市場信賴度，並可使具有特定意圖之產品無法進入我國市場，保障專網產品或 5G 設備基本安全性，提高 5G 環境資安體質。

(2) 建立組態合規轉譯檢測核心技術後，結合領域標準研析，如 GDPR、HIPAA 等，可使出口國際產品符合應用規範要求，強化國際市場競爭力。

(3) 利用導入 5G 自主技術(iMEC, vEPC, NFVI)，搭配資安協作優化效益，提供高服務品質且安全的服務環境，加速與 5G 產業鏈結，建構創新資安整合應用系統，確保在新型通訊發展的同時能確保安全防護。

2. 5G 資安產業化

(1) 結合國內資安業者整合本計畫資安防護模組，協助國內資安產業發展 5G 資安服務能量，進而提升國內資安廠商於新型通訊場域自主研發資安應用技術能量。

(2) 結合國內外開源社群共同協作，佈署資安協作平台，累積相關技術能量，推升產業生態發展，豐富網路型社會應用發展通訊系統軟硬體研發技術。

(3) 可協助資安業者跨入電信資安領域，而威脅驗證自動工具也創新服務項目與規模，對產業具有升級正面效益。

3. 參與人員專業訓練

電信營運商的安全防護正在改變以應對新的技術，5G 有望成為對電信業者具重要意義的技術，與企業相同，物聯網也讓電信業者面臨漏洞及規模問題，只是電信業者所遇到的規模問題會更大，而且在電信服務網路內出現後門漏洞所造成的不僅僅是資安風險的影響，還會影響品牌信譽及實體安全。本計畫研究人員於研究與實作資安偵測與防護過程中，學習並建立電信業等級的安

全防護及解決方案，孕育臺灣電信資安相關技術人才，同時帶動資安產業發展之外。

陸、自我挑戰目標

110 年度

1. 導入智慧製造 IEC62443 標準檢測至 5G 專網系統
2. 5G 資安防護系統整合於 3 個專網系統
3. 將 109 年度完成之 5G 資安防護模組，成功結合 5G+應用暨淬鍊之場域，導入 5G 資安防護機制 1 處以上

111 年度

1. 自動化工具除依據資安標準檢測合規程度外，將透過檢測所得到的資訊，評估 5G 元件風險，並可預警可能受高風險元件影響之服務。
2. 提供 5G 資安施作指引，並將自動化滲透技術於 3 個專網場域測試
3. 升級微網段隔離機制，強化整體系統保護。網路行為軌跡拓撲配對分析，提昇微網段隔離機制演算法
4. 提出之裝置辨識或威脅評估技術被 3 個專網所使用

柒、經費需求/經費分攤/槓桿外部資源

經費需求表(B005)

經費需求說明

5G 資安防護系統開發計畫規劃執行 4 年，110 年度計畫經費需求為 90,000 千元，皆為經常支出 90,000。無槓桿外部資源。

單位：千元

細部計畫名稱	計畫性質	110 年度			111 年度			112 年度			113 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
5G 資安防護系統開發計畫	4. 產業應用技術開發	90,000	90,000	0	90,000	90,000	0	90,000	90,000	0	90,000	90,000	0

110 年度經費需求表

經費需求說明

5G 資安防護系統開發計畫規劃執行 4 年，110 年度計畫經費需求為 90,000 千元，皆為經常支出(包含人事費 40,500 千元、材料費 732 千元、其它費用 48,768 千元)。無槓桿外部資源。

單位：千元

計畫名稱	計畫性質	預定執行機構	細部計畫重點描述	主要績效指標 KPI	110 年度						
					小計	經常支出			資本支出		
						人事費	材料費	其他費用	土地建築	儀器設備	其他費用
一、5G 資安防護系統開發計畫	4. 產業應用技術開發	經濟部技術處	• 發展智慧製造領域安全標準(IEC62443-4)之合規檢測技術。 • 研發多接取邊緣運算主動防禦機制，建立權限控管機制，並進行小規模誘捕介接大規模獵捕。 • 開發redundancy conflict與priorities conflict等兩種以上的衝突檢測與修正機制要	• 110年產出5G資安解決方案3 項以上 • 110 年聯合相關協會合作推廣5G 資安解決方案，至5G 產品上下游供應廠商3家 • 參與累計5個5G應用實驗場域進行5G 資安解決方案實證	90,000	40,500	732	48,768	0	0	0

			件，讓內嵌防護協作平台具備商業產品之穩定度。 • 針對5G專網虛擬和實體環境之各式日誌/事件/資源使用量指標等數據，研發數據解析器(parser)技術，建立數據標準化和一致化。 • 可互動檢視容器服務程序TCP/UDP連線關係與延遲、消耗頻寬等網路品質參數之界面工具。								

111 年度經費需求表

經費需求說明

5G 資安防護系統開發計畫規劃執行 4 年，111 年度計畫經費需求為 90,000 千元，皆為經常支出(包含人事費 40,500 千元、材料費 732 千元、其它費用 48,768 千元)。無槓桿外部資源。

單位：千元

計畫名稱	計畫性質	預定執行機構	細部計畫重點描述	主要績效指標 KPI	111 年度						
					小計	經常支出			資本支出		
						人事費	材料費	其他費用	土地建築	儀器設備	其他費用
一、5G 資安防護系統開發計畫	4. 產業應用技術開發	經濟部技術處	・ 發展智慧醫療領域標準HIPAA與HITECH合規檢測技術，並開發領域規範切換機制。 • 訂定5G專網資安施作指引，提供場域端於專網營運時的資安施作策略與方法。 ・ 強化Policy Interpreter與Security Enabler，使orchestration可以針對不同Layer的network policy做描述與轉譯，提高內嵌防護平台之產品價值與通用性。 ・ 針對5G專網虛擬和實體環境可得數據(日誌/事件/資源使用量指標)，建立行為模型和拓樸，及資源用量基線(baseline)。	• 111年產出累計5G資安解決方案5項以上 • 111 年累計6個5G垂直應用場域進行資安解決方案實證 • 111 年與業者合作5G 資安解決方案至5G 產品上下游供應廠商5家	90,000	40,500	732	48,768	0	0	0

			• 可主動學習服務常態服務品質規格，自動生成對應資安策略之管理工具。									

捌、儀器設備需求

(如單價 1000 萬以上儀器設備需俟受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 1000 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
110	無								
111	無								

玖、就涉及公共政策事項，是否適時納入民眾參與機制之說明

本計畫無涉及公共政策事項，不適用本章節。

拾、附錄

一、政府科技發展計畫自評結果(A007)

(一)計畫名稱：5G 資安防護系統開發計畫
審議編號：110-1401-09-20-04
計畫類別：前瞻基礎建設計畫

日期：109 年 3 月 29 日

(二)審查意見及回復：

序號	審查意見	回復說明
1	本計畫為第二期 5G 產業技術及應用發展計畫，因應 2019 年起國際 5G 商業網路陸續建設及創新商業服務推動，訂定計畫目標為(1)實現臺灣特色的 5G 自主垂直整合創新應用、(2)跨業合作帶動 5G 多元應用服務，淬鍊 5G 自主專網系統、(3)結合邊緣運算之 5G 新創應用、(4)健全 5G 資安能量。本計畫架構概分為 5G 垂直應用專網系統技術、全方位資安防護系統、科技整合創新應用、及系統整合及實地技術驗證等四分項，兼含技術研發及產業應用推動等作為。上述計畫架構及目標，部份依循前期計畫技研及產業應用主軸持續精進，並新增資安、應用服務、開源應用、即時視訊邊緣運算及產業生態鏈建構等工作，有利於推進我國 5G 產業發展及創新應用服務，計畫具備可行性。	謝謝委員對於本計畫所訂定之目標及執行之可行性給予肯定。配合計畫技術研發落至產業應用，已包含如：所開發之 AI 高精度視訊分析邊緣運算系統，並導入無人機場域、5G 資安防護系統結合 3 項國內網通產品，應用於醫療專網系統等。
2	前期計畫產業應用成果在技術移轉、委託及工業服務、促廠投資及衍生產值，均未能有所躍升。有鑑於此，本期計畫應詳實檢討技研標的之選擇、甚或技術功能規格目標，確認是否滿足國內主流產業鏈所需，並評析是否能因應國際大廠技術產品化腳步，以及是否能符合國際主流服務市場應用趨勢，另外，技研及應用服務導入時程擬定亦應確保可維持我國廠商技術及垂	謝謝委員意見，本計畫在技術面及產業應用成果皆有所提升，包含在技術面部分，將研發與布局 5G 技術、5G 專網、5G 資安、邊緣運算等關鍵智財，規劃訂定專利申請 100 件，專利獲證 40 件。在產業化面向上，規劃訂定技術移轉達 67,000 千元、技術服務 48,000 千

	直應用解決方案之競爭優勢。因此，在技研標的及垂直應用服務之選擇、功能規格目標之訂定、產業應用服務推廣之規劃、協助廠商切入主流市場應用，均應持續精進論述；在技研標的及垂直應用服務標的之選擇，亦可保持機動與彈性，進行必要的動態檢討及調整，以發揮資源運用的最大效益。另外，為彰顯各分、子項技術研發效益，在技術移轉、委託及工業服務、垂直應用服務之商轉效益及國際輸出、促廠投資等量化績效目標達成值，於年度成果報告應提出細項成效，以供查核追蹤技研成果之產業應用效益。	元，促成投資達 900,000 千元。另在質化的預期成果如下： 1. 建立 5G 小基站與 CPE 之完整射頻晶片智財，協助國內廠商推出自主之小基站晶片完整解決方案。 2. 提供 5G 專網系統一鍵安裝、5G 應用服務自動擴展、 5G 專網系統容錯與服務無縫升級等功能。 3. 透過資安 SI 廠商整合本計畫資安技術模組，選定利基應用領域，以提供 5G 資安解決方案予 5G 專網市場 4. 透過場域實證推動整合 5G 聯網無人機產業能量，共同發展契合使用需求與淬鍊 5G 聯網無人機垂直應用服務整體解決方案。 5. 棒球球賽賽事轉播雛型系統一套，可辨識多種棒球動作姿態、具備如同導播般的運鏡原則與自動化調整鏡位與角度。 6. 創造新型態我國技術自主之沉浸電競共感體驗服務，促成整體國內關聯產業(如轉播、直播主、遊戲製作等)。 7. 首創研發 5G Sniffer 設備，聆聽室內 5G 電波經人體反射後的變化，可以偵測睡眠者呼吸週期、呼吸中止事件、睡眠階段等。 與電腦、伺服器組裝業者合作，利用 5G 低延遲邊緣運算技術建構國際/國內首個用於改善工廠產線效率、錯誤率之正確性驗證。
3	資安除 Security 要考慮應用層的 Privacy。	透過符合 5G 垂直應用法規，先行滿足各領域之隱私需求，逐步從智慧製造(IEC62443)到醫療規範(HIPAA)，再依據歐盟 GDPR 與國際標準 ISO27701 強化隱私方面的檢測與動態監控技術，以確保 5G 專網之隱私安全。

4	計畫書撰寫宜加強: 資安項目可參考 NCC 近期將公佈之姿安管理框架及檢驗規範相關文件。	謝謝委員意見。本計畫已優化計畫書所需內容如下： 經瞭解 NCC 對電信業公告之「行動寬頻業務資通安全維護計畫」、「行動寬頻系統審驗技術規範草案之資通安全防護」，其檢驗規範與 3GPP SCAS 有重合之處，將持續追蹤進展，並反應到接續計畫之研發內容。

二、中程個案計畫自評檢核表

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)	V		V		(2)非延續性計畫 (3)非公共建設方案
	(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)		V		V	
	(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		V		V	
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」)		V		V	
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)		V		V	
	(2)是否研提完整財務計畫		V		V	
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)	V		V		
	(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		V		V	
	(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		V		V	
	(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	V		V		
	(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)		V		V	
	(6)屬具自償性者，是否透過基金協助資金調度		V		V	
5.人力運用	(1)能否運用現有人力辦理	V		V		

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	
	(2)擬請增人力者，是否檢附下列資料： a.現有人力運用情形 b.計畫結束後，請增人力之處理原則 c.請增人力之類別及進用方式 d.請增人力之經費來源		V		V	
6.營運管理計畫	是否具務實及合理性(或能否落實營運)	V		V		
7.土地取得	(1)能否優先使用公有閒置土地房舍		V		V	
	(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)		V		V	
	(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		V		V	
	(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		V		V	
	(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		V		V	
8.風險評估	是否對計畫內容進行風險評估	V		V		
9.環境影響分析 (環境政策評估)	是否須辦理環境影響評估		V		V	
10.性別影響評估	是否填具性別影響評估檢視表	V		V		
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	V		V		
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	V		V		
13.涉及空間規劃者	是否檢附計畫範圍具座標之向量圖檔	V		V		
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		V		V	
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		V		V	
	(2)是否檢附相關協商文書資料		V		V	
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		V		V	
	(2)是否規劃採用綠建築或其他節能減碳措施		V		V	

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	
	(3)是否檢附相關說明文件		V		V	
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	V		V		

主辦機關核章：承辦人 張智翔　　單位主管 何祥瑋　　首長

主管部會核章：研考主管　　會計主管　　首長

性別影響評估檢視表

【第一部分】：本部分由機關人員填寫

【填表說明】各機關使用本表之方法與時機如下：

一、計畫研擬階段

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

（二）請運用本表所列之評估項目，將性別觀點融入計畫書草案：

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

二、計畫研擬完成

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

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

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

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

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

計畫名稱：5G 資安防護系統開發計畫

主管機關（請填列中央二級主管機關）	經濟部	**主辦機關（單位）**（請填列擬案機關／單位）	經濟部技術處

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

評估項目	**評估結果**
1-1【請說明本計畫與性別平等相關法規、政策之相關性】 性別平等相關法規與政策包含憲法、法律、性別平等政策綱領及消除對婦女一切形式歧視公約（CEDAW）可參考行政院性別平等會網站（https://gec.ey.gov.tw）。	本計畫係以透過專業團隊執行 5G 專網資安技術研發，協助 5G 網通產品符合國際法規及建立專網威脅偵防系統，設計「性別平等政策綱領」內環境、能源與科技篇強調之消除

	職業性別隔離之精神，將鼓勵科技領域企業進用女性，吸引女性進入相關領域就業，且依據「經濟部性別平等推動計畫(108 至 111 年)」執行，業已遵循性別平等政策綱領、促進性別平等之基本精神。
評估項目	**評估結果**
1-2【請蒐集與本計畫相關之性別統計及性別分析（含前期或相關計畫之執行結果），並分析性別落差情形及原因】 請依下列說明填寫評估結果： a.歡迎查閱行政院性別平等處建置之「性別平等研究文獻資源網」 (https://www.gender.ey.gov.tw/research/)、「重要性別統計資料庫」(https://www.gender.ey.gov.tw/gecdb/)（含性別分析專區）、各部會性別統計專區、我國婦女人權指標及「行政院性別平等會–性別分析」(https://gec.ey.gov.tw)。 b.性別統計及性別分析資料蒐集範圍應包含下列 3 類群體： ①**政策規劃者**（例如:機關研擬與決策人員；外部諮詢人員）。 ②**服務提供者**（例如:機關執行人員、委外廠商人力）。 ③**受益者**（或使用者）。 c.前項之性別統計與性別分析應盡量顧及不同性別、性傾向、性別特質及性別認同者，探究其處境或需求是否存在差異，及造成差異之原因；並宜與年齡、族群、地區、障礙情形等面向進行交叉分析（例如：高齡身障女性、偏遠地區新住民女性），探究在各因素交織影響下，是否加劇其處境之不利，並分析處境不利群體之需求。前述經分析所發現之處境不利群體及其需求與原因，應於後續【1-3 找出本計畫之性別議題】，及【貳、回應性別落差與需求】等項目進行評估說明。 d.未有相關性別統計及性別分析資料時，請將「強化與本計畫相關的性別統計與性別分析」列入本計畫之性別目標（如 2-1 之ｆ）。	1.本計畫涉政策規劃者如下： 研擬與決策人員：因本計畫兼顧研發與應用，參與規劃及決策人員包含計畫主持人、協同計畫主持人、專案經理、產學研資深顧問及跨領域專家群等參與研擬方案之團隊包含男性 33 人(約 73.33%)，女性 12 人(約 26.67%)。 目前資通訊領域畢業生，女性人數僅占 3 成，致整體相關領域人才仍以男性居多。 未來仍將鼓勵更多女性人員參與，以促進兩性比例平衡。 2.本計畫涉服務提供者如下：因屬新興計畫(110-113年)，合作對象預計為網通業者、SI廠商、資安服務廠商或相關產業，未來在挑選服務提供者部分，將鼓勵女性人員參與，以促進兩性比例平衡。 3.本計畫涉受益者如下： 因屬新興計畫(110-113 年)，且以透過 5G 資安科技應用，協助

	製造業者、SI 廠商與資安服務業者為主，除符合產業資料管理與應用之需求外，辦理活動或推廣對象等亦將注意性別均衡性。
評估項目	**評估結果**
1-3【請根據 1-1 及 1-2 的評估結果，找出本計畫之性別議題】 性別議題舉例如次： **a.參與人員** 政策規劃者或服務提供者之性別比例差距過大時，宜關注職場性別隔離（例如：某些職業的從業人員以特定性別為大宗、高階職位多由單一性別擔任）、職場性別友善性不足（例如：缺乏防治性騷擾措施；未設置哺集乳室；未顧及員工對於家庭照顧之需求，提供彈性工作安排等措施），及性別參與不足等問題。 **b.受益情形** ①受益者人數之性別比例差距過大，或偏離母體之性別比例，宜關注不同性別可能未有平等取得社會資源之機會（例如:獲得政府補助；參加人才培訓活動），或平等參與社會及公共事務之機會（例如:參加公聽會/說明會）。 ②受益者受益程度之性別差距過大時（例如:滿意度、社會保險給付金額），宜關注弱勢性別之需求與處境（例如:家庭照顧責任使女性未能連續就業，影響年金領取額度）。 **c.公共空間** 公共空間之規劃與設計，宜關注不同性別、性傾向、性別特質及性別認同者之空間使用性、安全性及友善性。 ①使用性：兼顧不同生理差異所產生的不同需求。 ②安全性：消除空間死角、相關安全設施。 ③友善性：兼顧性別、性傾向或性別認同者之特殊使用需求。 **d.展覽、演出或傳播內容** 藝術展覽或演出作品、文化禮俗儀典與觀念、文物史料、訓練教材、政令/活動宣導等內容，宜注意是否避免複製性別刻板印象、有助建立弱勢性別在公共領域之可見性與主體性。 **e.研究類計畫** 研究類計畫之參與者（例如:研究團隊）性別落差過大時，宜關注不同性別參與機會、職場性別友善性不足等問題；若以	1.本計畫屬研究類計畫，研發計畫內容以推動產業創新研發為目的，如研發檢測工具、滲透測試工具與偵防模組，將透過技術移轉予網通廠商、資安服務業者、SI 廠商或相關產業，依據 95~107 年「經濟部科技研究發展經費及人力統計」之統計資料顯示女性投入比例為 28%，略低「經濟部性別平等推動計畫(108 至 111 年)」中，於任一性別不少於 1/3(約 33%)的性別目標，故本計畫將鼓勵更多理工背景之女性人員參與計畫。 2.承上，目前參與人員除規劃團隊外，如合作對象預計為網通廠商、資安服務業者、SI 廠商或相關產業，未來在挑選服務提供者部分，將鼓勵女性人員參與，以符合不同性別者之性別比例達 1/3 之目標。

「人」為研究對象，宜注意研究過程及結論與建議是否納入性別觀點。	

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

評估項目	評估結果
2-1【請訂定本計畫之性別目標、績效指標、衡量標準及目標值】 請針對 1-3 的評估結果，擬訂本計畫之性別目標，並為衡量性別目標達成情形，請訂定相應之績效指標、衡量標準及目標值，並納入計畫書草案之計畫目標章節。性別目標宜具有下列效益： **a.參與人員** ①促進弱勢性別參與本計畫規劃、決策及執行，納入不同性別經驗與意見。 ②加強培育弱勢性別人才，強化其領導與管理知能，以利進入決策階層。 ③營造性別友善職場，縮小職場性別隔離。 **b.受益情形** ① 回應不同性別需求，縮小不同性別滿意度落差。 ② 增進弱勢性別獲得社會資源之機會（例如:獲得政府補助；參加人才培訓活動）。 ③ 增進弱勢性別參與社會及公共事務之機會（例如:參加公聽會/說明會，表達意見與需求）。 **c.公共空間** 回應不同性別對公共空間使用性、安全性及友善性之意見與需求，打造性別友善之公共空間。 **d.展覽、演出或傳播內容** ① 消除傳統文化對不同性別之限制或僵化期待，形塑或推展性別平等觀念或文化。 ② 提升弱勢性別在公共領域之可見性與主體性（如作品展出或演出；參加運動競賽）。 **e.研究類計畫** ① 產出具性別觀點之研究報告。 ② 加強培育及延攬環境、能源及科技領域之女性研究人才，提升女性專業技術研發能力。 **f.**強化與本計畫相關的性別統計與性別分析。 **g.**其他有助促進性別平等之效益。	■有訂定性別目標者，請將性別目標、績效指標、衡量標準及目標值納入計畫書草案之計畫目標章節，並於本欄敘明計畫書草案之頁碼： 1.參與人員：將鼓勵更多理工背景之女性人員參與，以促進兩性比例平衡。 2.如有規劃辦理活動，亦將注意性別均衡性，如各性別參與度比例目標值為 1/3。 3.未來將建立性別統計與性別分析： (1)與廠商合作時，將蒐集廠商執行團隊成員之性別統計。 (2)配合經濟部辦理活動時，亦將進行參與者之性別統計分析，並蒐集回饋意見，以作為後續辦理活動之參考依據。 上述內容已納入計畫書草案。第 2-8~2-9 頁。 □未訂定性別目標者，請說明原因及確保落實性別平等事項之機制或方法。
評估項目	**評估結果**

2-2【請根據 2-1 本計畫所訂定之性別目標，訂定執行策略】

請參考下列原則，設計有效的執行策略及其配套措施：

a.參與人員

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

② 前項參與成員具備性別平等意識/有參加性別平等相關課程。

b.宣導傳播

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

② 宣導傳播內容避免具性別刻板印象或性別歧視意味之語言、符號或案例。

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

c.促進弱勢性別參與公共事務

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

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

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

④ 培力弱勢性別，形成組織、取得發言權或領導地位。

d.培育專業人才

① 規劃人才培訓活動時，納入鼓勵或促進弱勢性別參加之措施

（例如:提供交通接駁、臨時托育等友善服務；優先保障名額；培訓活動之宣傳設計，強化歡迎或友善弱勢性別參與之訊息；結合相關機關、民間團體或組織，宣傳培訓活動）。

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

③ 培訓內涵中融入性別平等教育或宣導，提升相關領域從業人員之性別敏感度。

■有訂定執行策略者，請將主要的執行策略納入計畫書草案之適當章節，並於本欄敘明計畫書草案之頁碼：

1.因本計畫核心為產業技術開發相關，將加強培育及延攬與5G 資安相關專業領域之女性研究人才，提升女性專業技術研發能力。

2.如有辦理相關活動，也將統計參加者人數及回饋意見之性別統計與性別分析，作為未來精進之參考。

3.本計畫目前參與人員除規劃團隊持續推動少數性別參與計畫外，未來如與廠商合作或配合經濟部辦理活動時，將鼓勵女性人員參與，希望藉由更多女性人員參與，促進兩性比例平衡，亦將進行性別統計分析，並蒐集回饋意見，以作為後續辦理活動之參考依據。

上述內容已納入計畫書草案。第 2-8~2-9 頁。

□未訂執行策略者，請說明原因及改善方法：

④ 辦理培訓活動之師資性別統計，作為未來師資邀請或師資培訓之參考。 **e.具性別平等精神之展覽、演出或傳播內容** ① 規劃展覽、演出或傳播內容時，避免複製性別刻板印象，並注意創作者、表演者之性別平衡。 ② 製作歷史文物、傳統藝術之導覽、介紹等影音或文字資料時，將納入現代性別平等觀點之詮釋內容。 ③ 規劃以性別平等為主題的展覽、演出或傳播內容（例如:女性的歷史貢獻、對多元性別之瞭解與尊重、移民女性之處境與貢獻、不同族群之性別文化）。 **f.建構性別友善之職場環境** 委託民間辦理業務時，推廣促進性別平等之積極性作法（例如：評選項目訂有友善家庭、企業托兒、彈性工時與工作安排等性別友善措施；鼓勵民間廠商拔擢弱勢性別優秀人才擔任管理職），以營造性別友善職場環境。 **g.具性別觀點之研究類計畫** ①研究團隊成員符合任一性別不少於三分之一原則，並積極培育及延攬女性科技研究人才；積極鼓勵女性擔任環境、能源與科技領域研究類計畫之計畫主持人。 ②以「人」為研究對象之研究，需進行性別分析，研究結論與建議亦需具性別觀點。	
評估項目	**評估結果**
2-3【請根據 2-2 本計畫所訂定之執行策略，編列或調整相關經費配置】 各機關於籌編年度概算時，請將本計畫所編列或調整之性別相關經費納入性別預算編列情形表，以確保性別相關事項有足夠經費及資源落實執行，以達成性別目標或回應性別差異需求。	□有編列或調整經費配置者，請說明預算額度編列或調整情形： ■未編列或調整經費配置者，請說明原因及改善方法： 本計畫訂定之性別目標及執行策略無涉費使用，未來仍將持續推動少數性別參與。

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

參、評估結果

<table>
<tr><td colspan="3">請機關填表人依據【第二部分－程序參與】性別平等專家學者之檢視意見，提出綜合說明及參採情形後通知程序參與者審閱。</td></tr>
<tr><td>3-1 綜合說明</td><td colspan="2">1. 本計畫經性別平等委員檢視後認為符合《性別平等政策綱領》中之〈環境能源科技篇〉之精神要旨。惟請明列參加本計畫之規劃及執行相關團體的性別統計，以了解其性別比例。
2. 本計畫已參採委員意見修正第一部分之性別影響評估檢視表評估內容。</td></tr>
<tr><td rowspan="2">3-2 參採情形</td><td>3-2-1 說明採納意見後之計畫調整（請標註頁數）</td><td>1. 本計畫原1.(1)與 1.(2)內容併為「本計畫涉政策規劃者如下：研擬與決策人員：因本計畫兼顧研發與應用，參與規劃及決策人員包含計畫主持人、協同計畫主持人、專案經理、產學研資深顧問及跨領域專家群等參與研擬方案之團隊包含男性33人，女性12人。
目前資通訊領域畢業生，女性人數僅占3成，致整體相關領域人才仍以男性居多。
未來仍將鼓勵更多女性人員參與，以促進兩性比例平衡。」（計畫調整如第10-8頁）
2. 本計畫兼顧研發與應用，參與規劃及決策人員包含計畫主持人、協同計畫主持人、專案經理、產學研資深顧問及跨領域專家群等參與研擬方案之團隊包含男性 33 人，女性 12 人。(計畫調整如第 10-8 頁）
3. 本計畫 2-1、2-2 之自評內容，均移至前項「有」訂定性別目標及訂定執行策略者之中，以符實際，並請將主要的執行策略納入計畫書草案之適當章節，並於本欄敘明計畫書草案之頁碼（如計畫書草案第 2-8~2-9 頁）。</td></tr>
<tr><td>3-2-2 說明未參採之理由或替代規劃</td><td>均已參採。</td></tr>
<tr><td colspan="3">3-3 通知程序參與之專家學者本計畫之評估結果：
已於 年 月 日將「評估結果」及「修正後之計畫書草案」通知程序參與者審閱。</td></tr>
</table>

- **填表人姓名：<u>張智翔</u> 職稱：<u>研究員</u> 電話：<u>(02)23946000#2583</u> 填表日期：<u>109</u>年<u>6</u>月<u>25</u>日**

【第二部分－程序參與】：由性別平等專家學者填寫

程序參與之性別平等專家學者應符合下列資格之一： □1.現任臺灣國家婦女館網站「性別主流化人才資料庫」公、私部門之專家學者；其中公部門專家應非本機關及所屬機關之人員（人才資料庫網址:http://www.taiwanwomencenter.org.tw/）。 □2.現任或曾任行政院性別平等會民間委員。 □3.現任或曾任各部會性別平等專案小組民間委員。	
（一）基本資料	
1.程序參與期程或時間	109 年 7 月 15 日 至 109 年 7 月 20 日
2.參與者姓名、職稱、服務單位及其專長領域	張瓊玲，臺灣警察專科學校教授兼海巡科主任，經濟部性別平等專案小組委員，性別平等政策綱領主筆人
3.參與方式	□計畫研商會議 □性別平等專案小組 ■書面意見
（二）主要意見（若參與方式為提報各部會性別平等專案小組，可附上會議發言要旨，免填 4 至 10 欄位，並請通知程序參與者恪遵保密義務）	
4.性別平等相關法規政策相關性評估之合宜性	合宜
5.性別統計及性別分析之合宜性	1.請將 1.(2)「均未指定單一性別參與」視實際情況改為「均有不同性別故同參與」 2.請明列參加本計畫之規劃及執行相關團體的性別統計，以了解其性別比例。
6.本計畫性別議題之合宜性	合宜
7.性別目標之合宜性	合宜
8.執行策略之合宜性	合宜
9.經費編列或配置之合宜性	合宜
10.綜合性檢視意見	1.請將本計畫 2-1、2-2 之自評內容，均移至前項：「有」訂定性別目標及訂定執行策略者之中，以符實際。 2.本計畫符合《性別平等政策綱領》中之〈環境能源科技篇〉之精神要旨，值得肯定。
（三）參與時機及方式之合宜性	合宜
本人同意恪遵保密義務，未經部會同意不得逕自對外公開所評估之計畫草案。 （簽章，簽名或打字皆可）__張　瓊　玲__	

三、政府科技發展計畫審查意見回復表(A008)

審議編號：110-1401-09-20-04
計畫名稱：5G 資安防護系統開發計畫
申請機關(單位)：經濟部技術處

序號	審查意見	回復說明	修正頁碼
1	本計畫應與經濟部 5G、物聯網、無人載具等相關計畫、及通傳會電信資安等相關計畫連結，擴大計畫成果的實質效益。	1. 本計畫成果規劃於經濟部 5G+系統暨應用淬鍊計畫之實驗場域，進行資安技術實證；同時協助 5G+與 B5G 科專計畫研發成果，做 5G 系統資安合規檢測與虛擬環境弱點盤點，並於系統維運期間，提供資安偵測和防護功能，確保產出元件符合國際標準與系統運行中的安全，擴大 5G 相關計畫之綜合效益 2. 為建立 5G 網路端到端的產品資安檢測，可結合物聯網系統檢測與驗證計畫成果之使用者裝置檢測能量，強化從使用者裝置到 5G 系統端資通安全性 3. 本計畫打造之資安技術及工具，可連結通傳會之電信資安計畫，協助提供相關資安審驗規範所需的工具，檢視 5G 公網資安之落實度驗證	1-5 2-5 2-7
2	本計畫應與電信業者合作，在 5G 商用公眾網路或專網網路進行落地測試，以驗證計畫成果。	5G 資安計畫成果落地對象涵蓋電信廠商、專網系統整合廠商與資安服務廠商等。針對電信業者提交通傳會之資通安全維護計畫，以及通傳會對電信業者的技術審驗規範中，包含業者對通傳會承諾達成之 5G 資安事項，如 5G 系統滲透測試、稽核 OSS（ Operations Support System）資料達成資安承諾事項；本計畫投入滲透測試工具研發，正與電信廠商洽談紫隊攻防演練，協助業者通過稽核；並打造 5G 系統 OSS 深度資料分析之安控洞察力與主動防禦技術，建構新形態威脅攻擊	3-6~3-8

		的防護網。此外，將與公網與專網廠商發展 5G 資安鑄造及創新資安服務模式，結合業者應用場域，進行垂直專網資安威脅建模與資安風險評估，並結合 5G 專網合規檢測技術與 5G 安控自動化防禦技術的技術，與資安業者發展專網資安解決方案。	

四、資安經費投入自評表(A010)

(如有填寫疑問，請逕洽行政院資安處 3356-8063)

部會			單位				
審議編號	計畫名稱	期程(年)	總經費(千元)(A)	資訊總經費(千元)(B)	資安經費(千元)(C)	比例[註1](D)	備註
110-1401-09-20-04	5G 資安防護系統開發計畫	110	90,000		90,000	100%	
	5G 資安防護系統開發計畫	111	90,000		90,000	100%	

資安經費投入項目				
項次	年度	投入項目類別[註2]	投入項目	預估經費(千元)
1	110	(A1)	5G 資安防護系統開發計畫	90,000
2	111	(A1)	5G 資安防護系統開發計畫	90,000
總計				

備註：

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

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

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

2、 投入項目類別請用下列代號填寫：

2-1 系統開發

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

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

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

2-2 軟硬體採購

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

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

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

2-3 其他建議項目

(3) 資安檢測標準研訂。

(4) 新興資安領域(例如：5+2產業創新計畫)之資安風險與防護需求研究。

(5) 新興資安領域之人才培育。

(6) 編撰資安訓練教材。

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

五、其他補充資料