政府科技發展中程個案計畫書

審議編號：110-1901-04-20-05

科技部工程司

「臺灣資安卓越深耕-學術型資安研究」

(核定本)

計畫全程期限：110 年 01 月至 114 年 08 月

目 錄

壹、基本資料及概述表(A003)

<table>
<tr><td>審議編號</td><td colspan="4">110-1901-04-20-05</td></tr>
<tr><td>計畫名稱</td><td colspan="4">臺灣資安卓越深耕-學術型資安研究</td></tr>
<tr><td>申請機關</td><td colspan="4">科技部工程司</td></tr>
<tr><td>預定執行機關
(單位或機構)</td><td colspan="4">科技部工程司、財團法人國家實驗研究院國家高速網路與計算中心</td></tr>
<tr><td rowspan="3">預定
計畫主持人</td><td>姓名</td><td>徐碩鴻</td><td>職稱</td><td>司長</td></tr>
<tr><td>服務機關</td><td colspan="3">科技部工程司</td></tr>
<tr><td>電話</td><td>02-2737-7524</td><td>電子郵件</td><td>shhsu@most.gov.tw</td></tr>
<tr><td>計畫摘要</td><td colspan="4">時代變遷與科技進步，IoT、5G、AI 等技術發展，使自駕車、無人機、智慧醫療、智慧零售、FinTech、智慧城市等自主系統應用日益普及；此些新興應用所採用的技術與機制相當複雜，因而產生許多潛在弱點；而駭客攻擊手法也從游擊戰，轉為具有策略、系統的團體戰，嚴重威脅我國邁向智慧國家的安全。有鑒於此，政府將「資安即國安」列為國家重大政策，「資安即國安 2.0 戰略」更著重提高人才培訓能量及開發資安創新技術；本計畫依循我國資安戰略，透過資安技術研發與機制設計，並培育資安研發人才，期能建立我國「資安自主研發」之厚實基礎。
本計畫規劃兩大分項計畫，包含工程司所推動之分項一「前瞻資安技術研究(Security in Air & Security on Chip)」與國研院國網中心推動之分項二「雲端資安攻防平台(CDX)」；針對未來在資訊科技上的應用情境，進行下一世代資安技術研發，如 IoT、5G & Beyond 5G、八大關鍵基礎建設（油、水、電、金融…等）、CPS 安全與工控、AI 系統防護、晶片製造、設計與架構安全等進行前瞻資安研究；經由研發技術及場域實戰淬鍊過程，培育資安技術研發人才之外，並藉由產學合作及技術移轉擴散資安研發能量，帶動國內資安產業技術升級與生態系建立；同時，透過移地研究、舉辦與參與國際會議與社群活動，掌握國內外資安技術發展趨勢與領先地位，鏈結與強化國際合作關係，以利提升我國資安技術水平。</td></tr>
<tr><td rowspan="3">計畫目標、預期關鍵成果及其與部會科技施政目標之關聯</td><td>計畫目標</td><td colspan="2">預期關鍵成果</td><td>與部會科技施政目標之關聯</td></tr>
<tr><td rowspan="2">O1 軟硬結合、資安創新</td><td colspan="2">KR1：針對未來新興應用軟硬體潛在資安威脅，開發對應前瞻創新資安防護技術。
*開發資安防護技術與機制 10 項/年。
*合作團隊(計畫)養成 5 群/年。
*產學合作 15 件/年，技轉與智財授權 3 件/年，總金額 600 萬/年。
*專利 5 件/全期程。</td><td rowspan="2">科技部:O1:鞏固自由探索研究環境，厚植科技立國能量;</td></tr>
<tr><td colspan="2">KR2：透過前瞻資安技術研發過程，強化軟硬體資安研發能量。</td></tr>
</table>

		*培育高階資安技術研發人才 200 人次/年。 *培訓資安專業實務人才 90 人次/年。	
	O2 資安場域、淬鍊技術	KR1：針對未來產業新興科技應用，進行特定領域資安實證場域研究。 *建置新興科技資安攻防實證場域 2 項/年。	科技部: O2:跨領域整合資源設施，提升研究資源綜效。 O3:強化科研應用與創新創業，完善科技創新生態圈。
		KR2：利用自建新興科技資安攻防實證場域，淬鍊特定領域資安技術。 *新興科技資安攻防專業實戰訓練 90 人次/年。 *新興科技資安攻防演練 1 場/年。	
	O3 國際接軌、共同合作	KR1：強化與先進國家資安研發機構合作關係，提高國內資安技術水平。 *先進國家移地研究 2 件/年。 *自主研發領先國際關鍵技術 2 項/年。	科技部:05:槓桿國際資源，活絡科研人才生態系;
		KR2：積極展現臺灣資安實力，提升我國資安領域能見度，掌握國內外資安技術發展趨勢與領先地位。 *邀請國際頂尖資安專家來台演講 3 場/年。 *舉辦大型國際資安會議 1 場/年。 *參與國際頂尖研討會發表論文 8 篇/年。	
預期效益	**一、強化未來新興科技資安防禦能量，確保智慧國家資訊安全** 投入新興應用軟硬體資安威脅防護前瞻研究，預備新型態威脅資安防護實力，深化高階資安研發人才的培育與產業資安防護能力，厚植我國資安自主研發能力，建構資訊安全環境，邁向智慧國家發展目標。 **二、帶動資安產業升級，建構資安產業聚落與生態體系** 整合跨域資安能量，由學研機構研發前瞻技術，法人與社群搭建技術移轉與擴散橋樑，產業夥伴合作進行技術落地，形成資安技術供給網路，提升國內資安產業研發技術水平，促進資安產業聚落與生態系的形成。 **三、提升國際能見度，建立國際資安研發領先地位** 積極爭取國際發表機會，展示臺灣資安實力，跨國攜手合作進行資安技術研究，汲取先進國家資安開發經驗，提高我國資安技術研發水平，挑戰開發全球領先資安技術。		
計畫群組及比重	□ 生命科技 ____ %　□環境科技 ____ %　□數位科技 ____ % ■ 工程科技 100 %　□人文社會 ____ %　□科技創新 ____ %		

<table>
<tr><td>計畫類別</td><td colspan="6">■ 前瞻基礎建設計畫</td></tr>
<tr><td>前瞻項目</td><td colspan="6">□ 綠能建設　■ 數位建設　□ 人才培育促進就業之建設</td></tr>
<tr><td>推動 5G 發展</td><td colspan="6">□ 是　■ 否</td></tr>
<tr><td>資通訊建設計畫</td><td colspan="6">□ 是　■ 否</td></tr>
<tr><td>政策依據</td><td colspan="6">一、PRESTSAIP-0106DG0601040000：數位國家・創新經濟發展方案：6.4 資通安全前瞻科技研發。
二、CSIDAP-20180202000000：資安產業發展行動計畫：2.研發關鍵技術。
三、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>計畫額度</td><td colspan="6">■ 前瞻基礎建設額度
110 年度 125,000 千元
111 年度 125,000 千元</td></tr>
<tr><td>執行期間</td><td colspan="6">110 年 01 月 01 日　至 111 年 12 月 31 日</td></tr>
<tr><td>全程期間</td><td colspan="6">110 年 01 月 01 日　至 114 年 08 月 31 日</td></tr>
<tr><td rowspan="2">前一年度預算</td><td>年度</td><td colspan="5">經費(千元)</td></tr>
<tr><td>109</td><td colspan="5">0</td></tr>
<tr><td rowspan="20">資源投入</td><td>年度</td><td colspan="5">經費(千元)</td></tr>
<tr><td>110</td><td colspan="5">125,000</td></tr>
<tr><td>111</td><td colspan="5">125,000</td></tr>
<tr><td>112</td><td colspan="5">100,000</td></tr>
<tr><td>113</td><td colspan="5">100,000</td></tr>
<tr><td>114</td><td colspan="5">50,000</td></tr>
<tr><td>合計</td><td colspan="5">500,000</td></tr>
<tr><td rowspan="5">110 年度</td><td>人事費</td><td>82,500</td><td>土地建築</td><td>0</td></tr>
<tr><td>材料費</td><td>19,000</td><td>儀器設備</td><td>2,500</td></tr>
<tr><td>其他經常支出</td><td>21,000</td><td>其他資本支出</td><td>0</td></tr>
<tr><td>經常門小計</td><td>122,500</td><td>資本門小計</td><td>2,500</td></tr>
<tr><td colspan="2">經費小計(千元)</td><td colspan="2">125,000</td></tr>
<tr><td rowspan="5">111 年度</td><td>人事費</td><td>82,500</td><td>土地建築</td><td>0</td></tr>
<tr><td>材料費</td><td>19,000</td><td>儀器設備</td><td>2,500</td></tr>
<tr><td>其他經常支出</td><td>21,000</td><td>其他資本支出</td><td>0</td></tr>
<tr><td>經常門小計</td><td>122,500</td><td>資本門小計</td><td>2,500</td></tr>
<tr><td colspan="2">經費小計(千元)</td><td colspan="2">125,000</td></tr>
<tr><td>中程施政計畫</td><td colspan="6">推動科研 4.5，營造友善研發環境，提升人才存量，躍升科研競爭力;</td></tr>
</table>

<table>
<tr><td>關鍵策略目標</td><td colspan="6"></td></tr>
<tr><td>本計畫在機關施政項目之定位及功能</td><td colspan="6">一、國家安全會議及行政院於105年召開「資安即國安策略會議」凝聚共識，以「打造安全可信賴的數位國家」作為戰略願景；行政院據此訂頒第五期「國家資通安全發展方案(106年至109年)」且規劃第六期「國家資通安全發展方案(110年至113年)」草案，為推升資安產業自主能量，行政院爰於106年召開「資安產業策略會議(SRB)」，並依會議結論擬訂「資安產業發展行動計畫(107年至114年)」。
二、本部為政府推動科學技術發展的專責機關，以支援學術研究為主要任務之一，於此主軸計畫「臺灣資安卓越深耕」中，協助發展學術型資安研究，以完備DIGI+及5+2產業創新方案資安能量。</td></tr>
<tr><td rowspan="6">計畫架構說明</td><td colspan="6">依細部計畫說明</td></tr>
<tr><td>細部計畫 1 名稱</td><td colspan="5">前瞻資安技術研究(Security in Air & Security on Chip)</td></tr>
<tr><td>110 年度
概估經費(千元)</td><td>98,000</td><td rowspan="2">計畫
性質</td><td rowspan="2">基礎研究</td><td rowspan="2">預定執行
機構</td><td rowspan="2">工程司</td></tr>
<tr><td>111 年度
概估經費(千元)</td><td>98,000</td></tr>
<tr><td>細部計畫
重點描述</td><td colspan="5">為了建立智慧國家發展之安全環境，本計畫以關鍵技術的研發為核心，透過未來產業的在資訊技術上的應用情境，例如：自駕車、無人機、智慧醫療、智慧零售、FinTech、智慧城市、晶片安全等議題，進行下一世代資安技術的研發。透過軟硬資安結合，提升資安防禦能量，了解並掌握目前科技前瞻技術與產業未來發展，透過產業鏈結與強化國際合作關係，提升我國資安技術能量，在分項計畫一的主要工作項目包含(1)開發軟體資安技術(Security in Air)，(2)開發硬體資安晶片(Security on Chip)。</td></tr>
<tr><td>主要績效指標
KPI</td><td colspan="5">1. 每年開發 10 項相關之前瞻關鍵資安技術與機制，產學合作案 15 件，技轉 3 件，總金額達 600 萬以上。
2. 每年培育高階資安技術研發人才 200 人次。
3. 每年參與國際頂尖研討會發表論文 8 篇。</td></tr>
<tr><td>細部計畫 2 名稱</td><td colspan="5">雲端資安攻防平台(CDX)</td></tr>
<tr><td>110 年度
概估經費(千元)</td><td>27,000</td><td>計畫
性質</td><td>基礎研究核心設施建置及維</td><td>預定執行
機構</td><td>國家高速網路與計算中</td></tr>
</table>

<table>
<tr><td rowspan="3"></td><td>111 年度
概估經費(千元)</td><td>27,000</td><td></td><td>運</td><td></td><td>心</td></tr>
<tr><td>細部計畫
重點描述</td><td colspan="5">本計畫整合跨領域資安能量，由學術單位建立前瞻技術，法人與社群搭建橋樑，也需與產業夥伴合作進行技術落地，形成資安技術供給網路。故分項二雲端資安攻防平台提供一個擬真的環境進行演練，雲端資安攻防平台(CDX)以虛擬化技術為基礎，改善傳統實體架構面臨的問題，例如：資源無法有效被利用、建置成本高昂、缺乏調度彈性等問題，建置出新一代的雲端平台。提供兩大主要的應用，分別是「資安實務人才培訓」以及「擬真場域攻防」。</td></tr>
<tr><td>主要績效指標
KPI</td><td colspan="5">1. 每年辦理資安攻防演練 1 場。
2. 每年資安專業實務人才培訓 90 人次。
3. 每年提供 450 萬核心小時進行資安人才培育。
4. 每年進行國際間攻防平台發展趨勢與功能分析，撰寫技術報告 1 份。</td></tr>
<tr><td>前一年計畫或相關之前期程計畫名稱</td><td colspan="6">全新的新興計畫，無相關前年（或前期）計畫</td></tr>
<tr><td>前期計畫或計畫整併說明</td><td colspan="6"></td></tr>
<tr><td>近三年主要績效</td><td colspan="6">全新的新興計畫，無相關前年（或前期）計畫</td></tr>
<tr><td rowspan="5">跨部會署計畫</td><td colspan="6">□ 是 ■ 否</td></tr>
<tr><td rowspan="2">合作部會署</td><td colspan="2" rowspan="2"></td><td>110 年度經費(千元)</td><td colspan="2"></td></tr>
<tr><td>111 年度經費(千元)</td><td colspan="2"></td></tr>
<tr><td>負責內容</td><td colspan="5"></td></tr>
<tr><td rowspan="2">合作部會署</td><td colspan="2" rowspan="2"></td><td>110 年度經費(千元)</td><td colspan="2"></td></tr>
<tr><td>111 年度經費(千元)</td><td colspan="2"></td></tr>
<tr><td>負責內容</td><td colspan="5"></td></tr>
<tr><td>中英文關鍵詞</td><td colspan="6">資通訊安全、晶片安全、前瞻研究、新興科技驗證場域、人才培育、國際合作。
security in air, security on chip, foresight research, emerging technology</td></tr>
</table>

	verification field, talents cultivation, international collaboration			
計畫連絡人	姓名	梁雁惠	職稱	助理研究員
	服務機關	科技部工程司		
	電話	02-27377525	電子郵件	yhliang@most.gov.tw

貳、計畫緣起

一、政策依據

1. PRESTSAIP-0106DG0601040000：數位國家‧創新經濟發展方案：6.4 資通安全前瞻科技研發。
2. CSIDAP-20180202000000：資安產業發展行動計畫：2.研發關鍵技術。
3. FIDP-20170201040000：前瞻基礎建設計畫：1.4 強化國家資安基礎建設。

二、擬解決問題之釐清

時代的變遷與科技進步，資訊科技與網路已成為各國關鍵基礎建設，關係國家競爭力根本和人民福祉。加上中美貿易戰影響全球經濟，工研院產科國際所指出，現在是發展「安全產業鏈」的重要契機，2019 年臺灣資安產業產值達新臺幣 437.3 億元，年增率 11.1%，預估 2020 年我國資安產值應可達成新台幣 550 億元的目標。

總統蔡英文上任後，即將「資安即國安」列為國家重大政策，全力填補我國在「資安機制」、「資安人才」、與「資安自主研發」的不足。因國內資安產業發展瓶頸主要在於市場規模太小，無法吸引專業人才投入，因此資安人員招募不易，資安廠商也難以在技術研發上深耕，試煉場域不足也無法提升服務品質問題，加上有越來越多的新型資安問題，如何防範並挑戰市場機會，需要有更多的學術研究預先投入，進行前瞻技術研究，並建置實戰淬鍊場域，透過產學合作提升我國資訊安全技術與人才能量，漸而帶動國內資安產業技術升級與生態系建立，確保我國智慧國家之資訊安全，提升我國資安能見度。

本計畫為鼓勵學研界針對資安議題投入前瞻關鍵技術研究，規劃兩大分項計畫，分項計畫一為「前瞻資安技術研究(Security in Air & Security on Chip)」，分項計畫二為「雲端資安攻防平台(CDX)」，計畫架構如圖 3.1 所示，執行機構包含科技部工程司和國家實驗研究院國家高速網路與計算中心。本計畫將整合產學研跨域軟硬體資安能量，發展對抗新型態攻擊之資安防禦技術，協助我國八大關鍵基礎設施，研發快速反應與防禦保護機制，提升產業資安防禦能量。建置資安攻防新興主題實測場域，促成資安攻防解決方案與新興智慧應用結合、發展跨域資安整體解決方案。

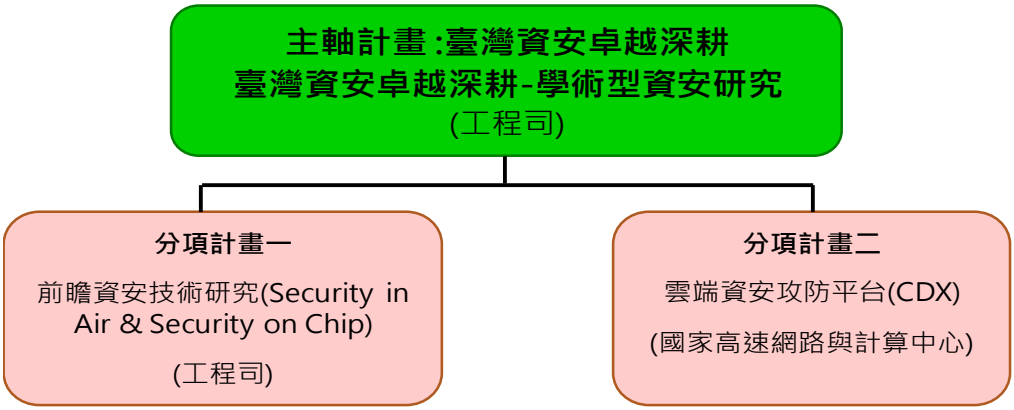

圖 3.1、計畫架構

為了建立智慧國家發展之安全環境，本計畫以關鍵技術的研發為核心，透過未來產業的在資訊技術上的應用情境，例如：自駕車、無人機、智慧醫療、智慧零售、FinTech、智慧城市、晶片安全等議題，進行下一世代資安技術的研發。透過軟硬資安結合，提升資安防禦能量，了解並掌握目前科技前瞻技術與產業未來發展，透過產業鏈結與強化國際合作關係，提升我國資安技術能量，在分項計畫一的主要工作項目包含(1)開發軟體資安技術(Security in Air)，(2)開發硬體資安晶片(Security on Chip)，分項計畫二的主要工作為(1)建構產業所需場域與攻防演練，(2)培訓跨領域資安人才，以下將進行詳細說明。

分項計畫一「前瞻資安技術研究(Security in Air & Security on Chip)」

1. 開發軟體資安技術(Security in Air)

預期未來在 5G 商轉後，整合 IoT、5G 及 AI 的相關技術應用，會被國內的公、私部門大量採用，相關技術也會應用到關鍵基礎設施的管理系統上。同時，這樣複雜的整合應用，也會產生新興的資訊威脅，將阻礙我國邁向智慧國家的發展。本計畫將透過確認未來在 IoT、5G 及 AI 等公、私部門的應用情境下，如自駕車、無人機、智慧醫療、智慧零售、FinTech、智慧城市等 IoT、5G、AI 等，可能會遭遇的資通訊安全問題，以及對關鍵基礎設施的資訊威脅，以研發與設計出下一個世代的前瞻資訊安全防護技術與機制。

當前 5G 位於起步階段，未來可以進行的商轉應用，除了提高當前 4G 應用的水準之外，也因為 5G 涉入雲端、行動裝置、車聯網等等領域，有可能會完全改變提供服務的軟硬體架構，各國對於 5G 資安防護的技術仍不成熟，是未來重要的資安議題。關鍵基礎設施的資安防護是資安議題的重中之重，隨著 5G 串聯 IoT 與 AI 新興技術與應用的出現，網路攻擊策略與技術也會不斷提升，對於關鍵基礎設施的資訊威脅也會不斷提升。AI 的技術現今已逐步融入日常生活中，如主動式行

車安全防護、個人化推薦服務等，因此，未來除了利用 AI 進行網路攻擊的威脅之外，駭客攻擊 AI 系統讓 AI 系統癱瘓或是從而控制 AI 系統將會成為資訊威脅的重心。當新興技術不斷投入產業界，傳統的網路安全防護技術也將面臨技術升級的課題，例如如何讓資安人員看見這些看不到的攻擊、應用區塊鏈特質進行資料防護、自動化資安資訊或提高警示的準確率以降低分析人力的需求等。

在 Security in Air 部份下，包含 4 個研究項目，分別為：(1) IoT, 5G & Beyond 5G、(2)關鍵基礎建設(油、水、電、金融等)、CPS 安全與工控、(3) AI 相關資安議題以及(4)網路安全(含區塊鏈等新興議題)，以回應上述未來我們即將面臨的資訊安全威脅，各項目詳述如下。

(1) IoT, 5G & Beyond 5G

第 5 代行動通訊（5th generation mobile networks, 5G）在通訊上具有 4G 所沒有的特性，也針對與物聯網技術以及人工智慧的應用，提出新型態的通訊方式、計算模型以及網路模型等，可支援更多開創性的應用。然而在未來的智慧 5G/B5G 的發展中，隨著各類智慧化終端裝置與邊緣計算裝置的數量大幅度的增加，異質性網路透過 5G/B5G 整合，使得資料分享的方式更為多元，以及因應應用而產生的計算需求也更為多樣化之下，產生了更多的資訊安全威脅以及防護的需求。

因應 5G 的蓬勃發展，目前已經有許多國家開始實際使用 5G 通訊，例如：韓國、美國、中國等國家，但也對應的衍生出許多問題和階段性不可避免的障礙和瓶頸。在 5G 的藍圖中，必須符合高頻寬、低延遲以及大量裝置連結這三項最主要的特性。以下就各國所遇到的情況大致以條列式進行簡單的國際現況之說明。

(1.1) 在高頻寬中，大部分國家所實際運行的 5G 系統都沒有辦法達到理想值 10Gbps 以上的速度，必須使用越高的頻率才能達到對應的速度，然而其所能覆蓋的範圍則會相對的縮小，進而導致必須以更大量的天線來滿足需求，也導致部分國家之通訊供應商為了擴大支援的範圍會降低其訊號所提供的速度。

(1.2) 由於各國對 5G 也都僅僅是剛起步的狀態下，基地台和天線的部件尚非常稀疏，僅僅是部分都市區域和較為核心的區塊能夠支援 5G，大部分的情況都還是會降階回 4G 的訊號，還甚至經常導致連線上的不穩定或沒有訊號。而目前參考文獻中有提到有對應方法可以主動將 5G 藉由基地台降階回 4G 的訊號，該部分也在 5G 的白皮書中也提到 5G 系統中會沿用 4G 的技術。這部分也會造成 5G 可能會產生 4G 原有的安全議題。目

前期望除實現攻擊的部分，並朝向抵禦該攻擊為最終目標。

(1.3) 在大量裝置連結中，5G 涵蓋了大部分的日常生活應用，包括交通上的自駕車系統。然而，目前有文獻發現可以利用晶片中含有硬體木馬來影響自駕車輔助系統的判斷機制，此攻擊也會造成相當程度的危害並嚴重威脅到使用者的生命財產之安全。因此，未來目標將朝向偵測硬體木馬存在的演算法。

本計畫將依循國際主流的 5G/B5G 通訊標準如 GSMA、3GPP 或 ITU-R 等，進行 5G/B5G 之無線存取網路與通訊網路的安全機制、攻擊偵測與自我修復、基礎設施硬體安全、結合物聯網與人工智慧所需的安全計算方法，以及基於 5G/B5G 的應用與服務的安全，並提出相關防護技術與安全機制。

(2) 關鍵基礎建設（油、水、電、金融）、CPS 安全與工控

國家關鍵基礎設施(Critical Infrastructure, CI)係指公有或私有、實體或虛擬的資產、生產系統以及網絡，此類設施倘因人為破壞或自然災害而受損，將影響政府及社會功能運作，造成人民傷亡或財產損失，進而引起經濟衰退、造成環境改變，甚或使國家安全及利益遭受損害，因此世界各國政府均重視關鍵基礎設施之發展與建設。

自上世紀 90 年代以來，國際上數起重大天然災害或人為攻擊事件，均嚴重影響關鍵基礎設施之正常運作，諸如美國 1995 年奧克拉荷馬州聯邦政府辦公大樓爆炸事件、1999 年 911 恐怖攻擊事件、2012 年 Sandy 颶風，日本 2011 年東北大震災、2016 年熊本震災、2018 年北海道震災、燕子颱風、西日本豪雨、2019 年哈吉貝颱風等災害，均造成關鍵基礎設施受損嚴重影響各國之經濟民生。因此國際間包括歐盟、加拿大、日本、澳洲等國，對關鍵基礎設施防護的概念，已從實體設施防衛與保護，轉變為要求提升整體設施功能與系統的耐災韌性，並期在事故發生後能夠快速恢復與持續運作。因此，關鍵基礎設施的防護重點將不僅僅只是針對實體建築物與設備，若是從持續運作的角度來看，更包括關鍵技術與人員，及關鍵基礎設施之資通訊與監視控制系統等設施。

因此關鍵基礎設施之資安防護，已成為世界各國在強化關鍵基礎設施防護中不可或缺並快速成長之一環，例如水資源領域方面，2011 年美國伊利諾州公共用水系統遭攻擊，2015 年烏克蘭水力發電系統遭受攻擊造成數十萬戶大停電，2019 年委內瑞拉水力發電受駭客網路攻擊造成全國規模的大停電；金融領域方面，駭客集

團企圖利用惡意程式攻擊全球逾 40 國家的銀行、電子支付系統與金融機構，估計已造成全球金融產業 10 億歐元的損失等，均顯示關鍵基礎設施資安防護之重要性所在。而就市場方面，Kenneth Research 於 2019 年 10 月研究報告指出，全球智慧電網資安市場規模在 2016 年為 44.5 億美元，預計 2025 年將成長至 110.6 億美元，更顯示關鍵基礎設施資安除為必要之環節外，同時亦有龐大之產業商機。

目前國際就關鍵基礎設施資通訊安全技術及設備方面，仍多係以共通之工業控制系統（Industrial Control Systems, ICS）架構作為資通安全防護之基礎思考模式，例如 NIST 之 SP800-82、IEC 之 62443-3-3 等資安防護基準；並基於此上開始建構獨特的關鍵基礎設施防護標準，諸如北美電力可靠度協會（North American Electric Reliability Corporation, NERC）提出之 CIP V5、美國核子管理委員會（Nuclear Regulatory Commission, NRC）提出之 RG5.71 等。

因此，本計畫擬建構、發展合乎目前國際共通性標準之資安防護技術與安全機制，並將相關技術與機制於關鍵基礎設施特有之場域環境進行實作，從而提出符合關鍵基礎設施特有防護需求之資安防護技術與防護基準。

(3) AI 相關資安議題

人工智慧技術興起之後，AI 已經被企業大量用於商業營運中，在資訊安全領域也不例外，如利用 AI 的學習技術，針對進入本地端的惡意流量的 behavior group 進行分析與萃取，了解惡意流量的行為模式，明確地定義這些 behavior group 的演算方法，透過評估其分類演算方法的精準性，調整相關參數以達成良好的防禦效果。上述的 AI 技術，也被應用到數位鑑識的領域中，例如利用 AI 對端點設備的行為資料側寫進行分類與標籤，最後自動產生分析報告。

然而，AI 技術本身也並非不會遭受攻擊。若駭客有能力取得或是找到 AI 系統的運作方式，就可以透過資料的操弄，引導 AI 系統做出自己想要的結果。以自駕車為例，自駕車透過鏡頭收集行車影像(圖 3.2)，並利用 AI 的影像識別技術確認當前的車道、號誌、標誌等等，來決定行車的方向與速度。然而，當駭客知道車道、號誌、標誌的訊號強度後，便能運用投影虛假的線條，讓自駕車誤判為車道從而影響車輛的行進方向。或是利用與標誌相近的符號或輪廓，讓自駕車誤判為速限標示，影響車輛的行車速度。

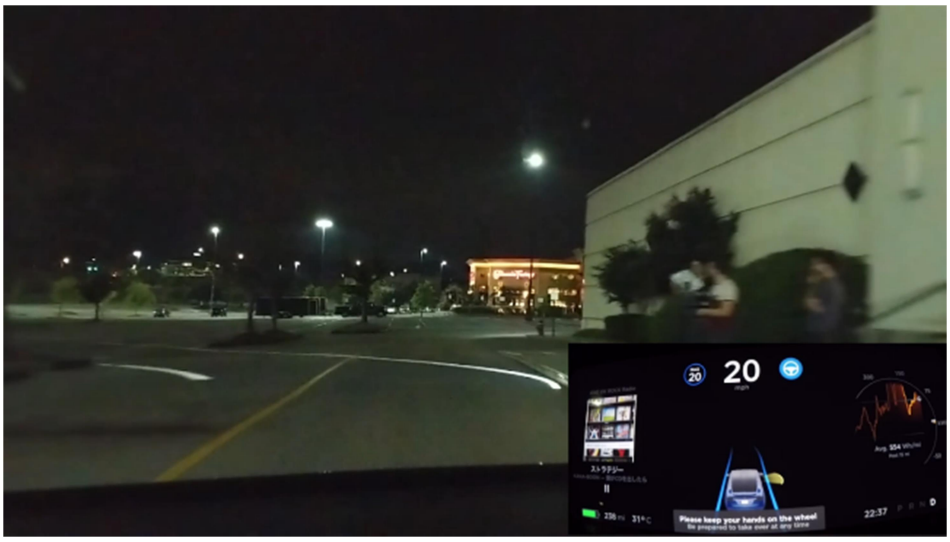

圖 3.2、誤導自駕車實驗

說明：研究人員利用在路面投影線條，成功影響自駕車行進的方向。資料來源：https://cyber.bgu.ac.il/how-a-300-projector-can-fool-teslas-autopilot/，Cyber@Ben-Gurion University of the Negev。

本計畫將著眼於 AI in Security 與 Security in AI 兩方面，一方面透過 AI 的技術，提升現有的資訊安全防禦技術的防禦率，以因應未來更為複雜的資安威脅。同時，對現有資安機制進行自主化，讓電腦能夠負擔大部分的人力工作，減輕資安人員的負擔，降低資安人力缺口的威脅。另一方面，發掘更多攻擊 AI 系統的威脅，並研發對應的防護技術或機制，建立 AI 應用的安全環境。

(4) 網路安全(含區塊鏈等新興議題)

隨著 AI、5G、物聯網技術的推展，各式各樣的自主系統不斷出現，例如智慧工廠、自駕系統等。這些系統的組成複雜，操控訊號也會在不同的設備中移轉，現有網路安全技術必須能夠應付如此複雜的環境，才能確保自主系統的安全。舉例來說，自動化系統含有大量的程式碼，如 Chevy Volt 一千萬行程式碼、美軍 UAV 飛控軟體三百五十萬航程式碼、波音 787 有六百五十萬行程式碼，以及我們日常所使用的 Google 瀏覽器也有一百萬行之譜，因這些具有高度複雜性，所以不管是在設計階段、實作階段、或是營運階段皆有可能引入非預期的錯誤與漏洞。同時，AI 技術的快速興起，也讓駭客創造出更強大的惡意工具，如利用 AI 的技術，偽造主管的電子郵件或 CEO 的聲紋進行進行社交工程、繞過圖像驗證技術、大量掃描系統漏洞等，必須擁有相關資安技術，因應這些先進網路武器，才能降低 AI 攻擊的

資訊威脅。

區塊鏈發展也從加密貨幣的應用，逐步滲透至其他產業之中，例如食品業的食品履歷、福斯汽車的供應鏈管理計畫、加拿大鋼鐵溯源管理計畫、日本音樂版權協會的版權管理計畫等。作為新興的數位工具，區塊鏈也可以應用在 IoT 上，對 IoT 裝置進行探查、偵測、紀錄、側寫等行為，建立 IoT 的資安防護機制。然而，區塊鏈並非沒有資安問題，雖然區塊鏈的去中心化與共識演算法，確保了資料不被竄改的安全性，但是資料透明的特性，讓區塊鏈必須使用加密方法來確保資料隱私，成為隱私防護的課題。另一方面，智能合約是人為撰寫的程式碼，是極有可能產生區塊鏈漏洞的部分，如何才能建立或設計一套安全機制，來偵測或降低智能合約的程式錯誤，確保區塊鏈不要產生資安漏洞。

本計畫參考國際現況擬定未來研發主題(表 3.1)，透過開發新興資安技術，或是整合現有資安技術，全面提升網路安全的防護，以因應未來各種資訊安全應用發展。

表 3.1、軟體資安技術研發主題與國際現況

研發主題	國際現況
IoT, 5G & Beyond 5G	1. 各國對 5G 也都是剛起步的狀態下，資安防範皆不成熟。 2. 5G 涵蓋了大部分的日常生活應用，若被駭客攻擊會造成相當程度的危害。
關鍵基礎建設（油、水、電、金融）、CPS 安全與工控	1. 國家關鍵基礎設施若遭受駭客攻擊，將造成人民傷亡或財產損失，進而引起經濟衰退。 2. 國際就關鍵基礎設施資通訊安全技術及設備方面，仍多係以共通之工業控制系統。
AI 相關資安議題	1. 透過 AI 等技術進行網路攻擊偵測，駭客也開始利用 AI 等技術進行攻擊。 2. 電子系統邁向 AIOT 裝置，資安防範刻不容緩。

網路安全(含區塊鏈等新興議題)	1. 電腦犯罪手法日新月異且日益複雜，資訊資產不受到有意或無易地洩漏、破壞、假造，以及未經授權的獲取、使用、修改。 2. 透過區塊鏈系統本身的安全防護機制，或應用區塊鏈系統上的資訊安全防護機制。 3. 整合安全機制並擴展新興資安產業。

2. 開發硬體資安晶片(Security on Chip)

隨著時代變遷與科技進步，全球 IoT、AI 等技術快速演進與 5G 世代來臨，使現代生活發展趨向自動化及智慧化。根據市場研究機構 IHS Markit 預測，到 2025 年可連網裝置將超過 750 億台，如此大量的連接裝置可拉進人與人、人與物的距離，並提供更多管道搜集大數據資料，但便利同時也伴隨著隱憂，連接網路會讓這些裝置暴露在風險中，資安威脅大幅增加。由於這些新興應用採用的技術與機制相當複雜，因而產生許多潛在弱點與安全漏洞，讓駭客可能藉此入侵竊取個資或企業機密資料。近年各種資安攻擊事件時有耳聞，對資訊安全的防護可說是未來科技發展所需克服的極大難題與挑戰。

關於資訊安全性討論方向主要可概分為軟體與硬體兩大類，近來各項新興技術應用對硬體安全性需求正高速增長。以目前蓬勃發展中的 IoT 應用為例，其架構涵蓋多種軟硬體整合，包括晶片、記憶體、傳輸介面、通訊協定、應用程式及雲端平台等各種異質系統，若只利用軟體方式提供安全防護，已不足以防範層出不窮的資安威脅。之前揭露的 OpenSSL 旁通道攻擊漏洞就是一例，只要在附近用電磁波接收物理訊號，就可以獲得其加密金鑰；另外像是 2018 年 Nvidia 晶片漏洞禍及任天堂 Switch，以及近期造成熱烈討論的 Intel 與 AMD CPU 的安全漏洞等案例，皆是硬體安全議題最佳實證。據報導指出，單只 2018 整年就有超過 30 億各類系統晶片因硬體攻擊，遭受資料盜竊、綁架設備和其他安全性威脅。未受保護硬體可能威脅系統安全、可靠性和效能，讓廠商遭到財務和形象損失，甚至讓使用者暴露於危險之中，嚴重影響我國技術發展與資訊安全。

2019 年政府將「資安即國安」列為國家重大政策，加速研提「資安即國安 2.0 戰略」，顯示我國刻不容緩全力發展資安技術的決心。我國長期身為半導體設計與製造重鎮，上中下游產業鏈整合完整，擁有厚實的研發實力與提高技術在市場應用時效等多重優勢。爰此，本計畫依循我國資安戰略，針對硬體安全防護技術研發，

規劃「Security on Chip」主軸，期能透過本計畫運作結合我國半導體產業優勢，加速關鍵技術研發進程，帶動國內資安產業技術升級與生態系建立，進而成為整體產業推動發展最堅實的後盾。

現今晶片設計與生產流程十分龐大而複雜，為增進效率，業界藉由全球化專業分工以降低製造成本，其過程至少牽涉到 IC 設計公司、設計自動化工具(EDA)供應商、矽智財供應商、設計服務公司、晶圓代工廠及封裝測試廠…等，每顆晶片都可能是全球不同公司團隊的合作結晶。晶片製作是一步步累積的過程，每個步驟都不能省略，高度化分工可以解決和減緩設計生產成本，但也讓安全議題浮出檯面。換言之，IC 在設計或製造過程中都有可能被惡意改變電路、植入硬體木馬(Hardware Trojan)，或是管理不慎、機密外流、設計失誤等，都會造成整體安全漏洞，使每個步驟都可能面臨攻擊，成為重大資安破口。

分項計畫二「雲端資安攻防平台 (CDX)」

本計畫整合跨域資安能量，由學術單位建立前瞻技術，法人與社群搭建橋樑，也需與產業夥伴合作進行技術落地，形成資安技術供給網路。故分項二雲端資安攻防平台提供一個擬真的環境進行演練，雲端資安攻防平台(CDX) 以虛擬化技術為基礎，改善傳統實體架構面臨的問題，例如：資源無法有效被利用、建置成本高昂、缺乏調度彈性等問題，建置出新一代的雲端平台。提供兩大主要的應用，分別是「資安實務人才培訓」以及「擬真場域攻防」，以下進行詳細說明：

「資安實務人才培訓」以演練的環境為發展重點，提供學員在進行資安課程時，可以擁有安全可控的練習環境，在網路架構部份則採用虛擬隔離的技術，可確保資安攻防過程中產生的惡意行為，不會影響到真實營運的網路環境。透過研究歷年存在於真實生活的重大資安事件(例如：WannaCry、Citrix 等等)，於 CDX 中部署相關的弱點環境，提供用戶隨選漏洞(Vulnerability on Demand, VOD)的服務，以讓用戶體驗更貼近真實情況的弱點驗證與實作環境。此外，建置擬真企業網路環境，搭配歷年資安弱點環境及虛擬資安防護設備，提供更貼近企業實際環境的攻防演練場域，並透過實兵演練方式驗證資安防護機制是否完善，同時亦可提升業界人員資安防禦技術之能力。

在「擬真場域攻防」發展過程，在過去幾年來，運用發展之雲端資安攻防平台，提供國內資訊安全人才培訓環境，辦理教育訓練及成果研討會等推廣活動，包含：

辦理至少 20 場推廣活動、4 場全國大型競賽活動，涵括主機堡壘賽、IoT 裝置、情境場域、產品測試、藍隊防守等類型，參加人次達 723 人以上，其中 2019 年的 iThome 臺灣資安大會上更使用於 Blue Team Workshop 中，相較於 Cyber Range、Cyber Bit 等資安教育訓練平台為國外研發國內代理的產品，CDX 是唯一國產的資安教育訓練平台。2018 年更獲總統府資安週及行政院資安週邀請，報告予總統及行政院各長官。並協辦成大 TWISC T 貓盃、金象盃，技服中心金盾獎出題，及提供平台予資安人才培育計畫 MyFirst CTF 等資安競賽。

三、目前環境需求分析與未來環境預測說明

（一）全球資訊安全推動現況

1. 主要國家推動策略

(1) 以色列：透過軍中帶頭推動國家資安發展，以色列 8200 部隊是以色列國防軍中規模最大的獨立軍事單位，透過資訊化創新部隊進行嚴格培訓與研發。政府也投入 5 億美元進行強力推動以建立網路安全生態系統」，隨時注意與掌握網路安全與新興技術在產業與市場動態。

(2) 韓國：韓國政府以預算無上限的方式進行資安推動，建構資安產業良性發展的架構及打造強化全球競爭力的生態體系。以「K-ICT Security 2020」規劃，設定 2020 年扶植資訊安全產業發展：(1)「透過強化資訊安全產業基礎去創造未來成長動力」、(2)「開發可取得市場先進者優勢的原始技術」，(3)「精銳資訊安全人才養成和資訊安全實踐文化建設」，以及(4)「提高網路資訊安全復原力所需資金的擴大」。

(3) 日本：2018 年 7 月 27 日公布網路安全戰略，主要目的係持續實現「提昇經濟社會活力與永續發展」、「實現國民安全且安心生活之社會」、「維持國際社會和平、安定與保障日本安全」三大目標。利用先進技術支持創新網路安全業務，制定網路安全措施指南，並對物聯網網路攻擊從不同角度進行劃分來採取措施，並透過國際合作與標準化來達到安心生活的社會。

(4) 美國：由國土安全委員會批准於 2018 年通過「關鍵基礎設施資安防護法案」，在強化關鍵基礎設施系統抵禦網路攻擊能量與技術法案。幫助識別工業控制系統相關威脅，從而將國土安全部保護這些系統的工作

任務法制化，並帶頭協調及處理跨關鍵基礎領域部門網路安全事件。2019 年通過「政府協助企業資安防護法案」，協助政府機關及私人企業避免網路攻擊，在這些組織遭到攻擊時也應協助緩解。

(5) 德國：透過官方 BMBF 推動資訊科技安全研究計畫之一數位生活之資訊自主權與安全，計畫目標為致力於開發使用者導向之保護個人資料隱私與新興技術之安全解決方案。

(6) 荷蘭：荷蘭擁有全歐洲最大的資安產業聚落，透過情報、教育、訓練及新創，建立國家安全、都市安全、資訊安全、刑事及關鍵基礎設施防護的五大領域之專業能量。

（二）未來我國資訊安全發展趨勢

時代的變遷與科技進步，資訊科技與網路已成為各國關鍵基礎建設，關係國家競爭力根本和人民福祉。加上中美貿易戰影響全球經濟，工研院產科國際所指出，現在是發展「安全產業鏈」的重要契機，2019 年臺灣資安產業產值達新臺幣 437.3 億元，年增率 11.1%，預估 2020 年我國資安產值應可達成新台幣 550 億元的目標。

總統蔡英文上任後，即將「資安即國安」列為國家重大政策，全力填補我國在「資安機制」、「資安人才」、與「資安自主研發」的不足。因國內資安產業發展瓶頸主要在於市場規模太小，無法吸引專業人才投入，因此資安人員招募不易，資安廠商也難以在技術研發上深耕，試煉場域不足也無法提升服務品質問題，加上有越來越多的新型資安問題，如何防範並挑戰市場機會，需要有更多的學術研究預先投入，進行前瞻技術研究，並建置實戰淬鍊場域，透過產學合作提升我國資訊安全技術與人才能量，漸而帶動國內資安產業技術升級與生態系建立，確保我國智慧國家之資訊安全，提升我國資安能見度。

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

本計畫將整合產學研跨域軟硬體資安能量，發展對抗新型態攻擊之資安防禦技術，協助我國八大關鍵基礎設施，研發快速反應與防禦保護機制，提升產業資安防禦能量。建置資安攻防新興主題實測場域，促成資安攻防解決方案與新興智慧應用結合、發展跨域資安整體解決方案。本計畫對各層面的影響說明如下:

1. 產業技術面：研發 IoT、5G、AI、網路安全、關鍵基礎設施、晶片安全關鍵模組之安全技術與防護機制，奠定我國資安技術發展良好基石。
2. 人才培育面：培育國內 5G、IoT、AI、網路安全、關鍵基礎設施、晶片安全資安跨域人才。
3. 產業面：強化我國資安產業生態系在 IoT、5G、關鍵基礎設施、AI、晶片安全等資安技術之升級。

參、計畫目標與執行方法

一、目標說明

政府將「資安即國安」列為國家重大政策，「資安即國安 2.0 戰略」更著重提高人才培訓能量及開發資安創新技術。本計畫也因應越來越多的新型資安問題，鼓勵更多學術老師投入資訊安全領域，計畫目標為：

1. 軟硬結合、資安創新

針對關鍵基礎可能遭遇的資訊威脅，找出未來可能遭遇的資通訊威脅，開發相對應前瞻資安防護技術。

2. 資安場域、淬鍊技術

配合台灣產業，強化產業軟硬體場域，進行學術與產業人才的資安培訓。

3. 國際接軌、共同合作

資安為當前國際性之重要研究、開發與產業議題，透過至國際先進資安研發單位進行移地研究，與共同研究或開發資安技術與機制，有利於提高我國在資安領域之國際地位與技術水平。

計畫全程總目標					
1. 軟硬結合、資安創新 2. 資安場域、淬鍊技術 3. 國際接軌、共同合作					
年度	第一年 民 110 年	第二年 民 111 年	第三年 民 112 年	第四年 民 113 年	第五年 民 114 年
年度目標	1. 與產業界共同擬定安全晶片關鍵模組。 2. 研發對應之基本可行的資安防護技術與安全機制。 3. 培育關鍵資安技術研發人才與晶片資安研發人才。 4. 完成 Blue Team、Red Team Offense 等產業場域研	1. 發展國際共通性關鍵基礎設施防護規範。 2. 開發 IoT、5G 及 AI 等應用之資安工具。 3. 完成關鍵模組效能及旁通道攻擊之晶片驗證分析。 4. 培育關鍵資安技術研發人才與晶片資安研發人才。 5. 完成 IoT、	1. IoT、5G 及 AI 等應用資安技術落地驗證。 2. 資安技術與安全機制之研究成果推廣。 3. 關鍵模組設計效能驗證，並與業界實際系統搭配。 4. 提出後量子密碼演算法層級解決方案。 5. 培育關鍵資安技術研發	1. IoT、5G 及 AI 等應用資安技術落地驗證與成果推廣。 2. 提出應用國際開源的晶片安全框架技術。 3. 實現關鍵模組於業界 IoT、5G 等應用(單一 TEE 執行環境)。 4. 提出後量子密碼解決方案及其硬體架構實現，參與 NIST 提	1. 資安技術產業化，推動資安領域創新創業。 2. 推動資安產業聚落與生態系成形。 3. 資安技術落地驗證與成果推廣。 4. 培育關鍵資安技術研發人才與晶片資安研發人才。 5. 完成 Medical Hacking 產業場域研究。 6. 培訓跨領域

	究。 5. 與企業合作辦理資安競賽，進行實證場域攻防演練。 6. 與產業進行產學合作，促進國內跨領域產業升級。	Bank Hacking 等產業場域研究。 6. 與企業合作辦理資安競賽，進行實證場域攻防演練。 7. 與產業進行產學合作，促進國內跨領域產業升級。	人才與晶片資安研發人才。 6. 完成 Social Engineering 產業場域研究。 7. 培訓跨領域資安人才。 8. 與產業進行產學合作，促進國內跨領域產業升級。	案。 5. 培育關鍵資安技術研發人才與晶片資安研發人才。 6. 完成 Car Hacking、Health-care Hacking 等產業產業場域研究。 7. 培訓跨領域資安人才。 8. 與產業進行產學合作，促進國內跨領域產業升級。	資安人才。 7. 與產業進行產學合作，促進國內跨領域產業升級。
預期關鍵成果	1. 開發 10 項相關之前瞻關鍵資安技術與機制，產學合作案 15 件，技轉 3 件，總金額達 600 萬以上。 2. 培育高階資安技術研發人才 200 人次。 3. 參與國際頂尖研討會發表論文 8 篇。 4. 辦理資安攻防演練 1 場。 5. 資安專業實務人才培訓 90 人次。 6. 提供 450 萬核心小時進行資安人才培育。	1. 開發 10 項相關之前瞻關鍵資安技術與機制，產學合作案 15 件，技轉 3 件，總金額達 600 萬以上。 2. 培育高階資安技術研發人才 200 人次。 3. 參與國際頂尖研討會發表論文 8 篇。 4. 辦理資安攻防演練 1 場。 5. 資安專業實務人才培訓 90 人次。 6. 提供 450 萬核心小時進行資安人才培育。	1. 開發 10 項相關之前瞻關鍵資安技術與機制，產學合作案 12 件，技轉 3 件，總金額達 600 萬以上。 2. 培育高階資安技術研發人才 180 人次。 3. 參與國際頂尖研討會發表論文 8 篇。 4. 辦理資安攻防演練 1 場。 5. 資安專業實務人才培訓 67 人次。 6. 提供 333 萬核心小時進行資安人才培育。 7. 進行國際間	1. 開發 10 項相關之前瞻關鍵資安技術與機制，產學合作案 12 件，技轉 3 件，總金額達 600 萬以上。 2. 培育高階資安技術研發人才 180 人次。 3. 參與國際頂尖研討會發表論文 8 篇。 4. 辦理資安攻防演練 1 場。 5. 資安專業實務人才培訓 67 人次。 6. 提供 333 萬核心小時進行資安人才培育。	1. 產學合作或技術移轉案 6 件，總金額達 300 萬以上。 2. 培育高階資安技術研發人才 40 人次。 3. 資安專業實務人才培訓 33 人次。 4. 提供 167 萬核心小時進行資安人才培育。 5. 進行國際間攻防平台發展趨勢與功能分析，撰寫技術報告 1 份。

	7. 進行國際間攻防平台發展趨勢與功能分析，撰寫技術報告1份。	7. 進行國際間攻防平台發展趨勢與功能分析，撰寫技術報告1份。	攻防平台發展趨勢與功能分析,撰寫技術報告1份。		

二、執行策略及方法

細部計畫名稱	執行策略說明
前瞻資安技術研究(Security in Air & Security on Chip)	(1) 開發軟體資安技術(Security in Air) ● 針對 5G(B5G)、CI、IoT 與 AI 等相關應用潛在威脅，開發對應前瞻資安防護技術 ● 開發先進資安技術與防護機制，培育資安研發人才，建立資安研發自主能量 ● 研發成果擴散產業界，帶動國內資安產業發展 ● 建立資安技術自主創新,提高資安研發人才供給，帶動資安產業升級,推動資安產業聚落與生態系的形成與發展 (2)開發硬體資安晶片(Security on Chip) ● 即時掌握最新國際規範並參與國際競賽及提案 ● 透過 PUF 技術以加強晶片安全防護 ● 開發基於安全設計的 EDA 工具與環境 ● 針對各式旁通道攻擊提出防禦機制 ● 應用國際開源的晶片安全框架技術
雲端資安攻防平台 (CDX)	● 資安師資實務培訓環境應用開發 ● 新興科技擬真攻防場域開發 ● 資安人才培育資源擴充與功能開發

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、 資安專任人力招聘與續留困難，目前暫以研究生人力補足人力缺口。

2、 將來預計透過不同的人才培育模式建立專業人物、人才、人手，擴大到產業人才培訓等，逐步建立資安人才生態系。

3、 本計畫積極落實性別平等教育與性別平等教育白皮書之規劃，鼓勵學生適性揚才。

四、與以前年度差異說明

年度 差異項目	107 年度	108 年度	109 年度	110-111 年度

本計畫無

五、跨部會署合作說明

本計畫無

肆、近三年重要效益成果說明

本計畫無

伍、預期效益及效益評估方式規劃

1.預期效益

(1)技術面：研發 IoT、5G、AI、網路安全、關鍵基礎設施、晶片安全關鍵模組之安全技術與防護機制，奠定我國資安技術發展良好基石。

(2)人才面：培育國內 5G、IoT、AI、網路安全、關鍵基礎設施、晶片安全資安跨領域人才。

(3)產業面：強化我國資安產業生態系在 IoT、5G、關鍵基礎設施、AI、晶片安全等資安技術之升級。

2.效益評估方式規劃：

(1)技術面：

(1.1)因技術開發屬於前瞻技術，則以申請專利數、專家學者引用與評估等方式評估。

(1.2)由產學研專家委員依據本計畫之研發成果，評估是否為我國之關鍵資訊安全技術或防護機制。

(1.3)掌握後量子密碼學衍生之相關演算法與硬體實作，參與美國 NIST 提案，提升我國技術能見度。

(2)人才面：

(2.1)由本計畫培育之博碩士生、博士後研究員及研究助理之人才數目，以及相關研究成果發表於資安領域國際期刊、研討會、邀至國際活動演講(如以色列資安週)或參加資安競賽名次進行評估。

(2.2)由本計畫所培訓之跨領域資安人才之數量以及參與資安競賽活動之人數，評估此計畫協助國內學界及業界培植資安人才。

(3)產業面：

(3.1)透過產學合作件數、技術轉移件數、業者投入資金、投入人力進行評估。

(3.2)由團隊與業界合作廠商數目、合作方式、實證場域攻防演練參加人數、資安技術論壇場數，評估是否達成產業效益目標。

(3.3)將 CDX 導入資安業者產品，了解企業使用率與下載數，評估產業在功能與安全性驗證。

陸、自我挑戰目標

110 年度

1. 制定 IoT、5G、AI、網路安全、關鍵基礎設施、晶片安全、後量子演算法等相關之關鍵資訊安全技術與防護機制之國際標準。
2. 培育頂尖人才以吸引國際大廠來台設立資訊安全研發中心。
3. 與 5 間國內外資安廠商合作，將產品導入至 CDX 實戰場域中，以協助進行產品功能及安全性的驗證。
4. 與產業界共同擬定安全晶片關鍵模組。
5. 研發對應之基本可行的資安防護技術與安全機制。
6. 培育關鍵資安技術研發人才與晶片資安研發人才。
7. 爭取國際知名資安研討會來台舉辦。
8. 與國內廠商共同舉辦台灣資安週活動。

111 年度

1. 發展國際共通性關鍵基礎設施防護規範。
2. 開發 IoT、5G 及 AI 等應用之資安工具。
3. 完成關鍵模組效能及旁通道攻擊之晶片驗證分析。
4. 培育關鍵資安技術研發人才與晶片資安研發人才。
5. 促成國內學者加入國際頂級資安研討會議程委員，如 IEEE Symposium on Security and Privacy、ACM Conference on Computer and Communications Security、USENIX Security Symposium 等。
6. 與國內廠商共同舉辦台灣資安週活動。

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

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			114 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	小計	經常支出	資本支出
細部計畫 1:前瞻資安技術研究(Security in Air & Security on Chip)	基礎研究	98,000	98,000	0	98,000	98,000	0	80,000	80,000	0	80,000	80,000	0	40,000	40,000	0
細部計畫 2:雲端攻防演練平台(CDX)	基礎研究核心設施建置及維運	27,000	24,500	2,500	27,000	24,500	2,500	20,000	18,000	2,000	20,000	18,000	2,000	10,000	9,000	1,000

110 年度經費需求表

經費需求說明

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、細部計畫 1 前瞻資安技術研究(Security in Air & Security on Chip)	基礎研究	工程司	1. 與產業界共同擬定安全晶片關鍵模組。 2. 研發對應之基本可行的資安防護技術與安全機制。 3. 培育關鍵資安技術研發人才與晶片資安研發人才。	1. 每年開發 10 項相關之前瞻關鍵資安技術與機制，產學合作案 15 件，技轉 3 件，總金額達 600 萬以上。 2. 每年培育高階資安技術研發人才 200 人次。 3. 每年參與國際頂尖研討會發表論文 8 篇。	98,000	74,000	12,000	12,000	0	0	0

二、細部計畫 2 雲端資安攻防平台(CDX)	基礎研究核心設施建置及維運	國家高速網路與計算中心	1. 完成 Blue Team、Red Team Offense 等產業場域研究。 2. 與企業合作辦理資安競賽，進行實證場域攻防演練。 3. 與產業進行產學合作，促進國內跨領域產業升級。	1. 每年辦理資安攻防演練 1 場。 2. 每年資安專業實務人才培訓 90 人次。 3. 每年提供 450 萬核心小時進行資安人才培育。 4. 每年進行國際間攻防平台發展趨勢與功能分析，撰寫技術報告 1 份。	27,000	8,500	7,000	9,000	0	2,500	0

111 年度經費需求表

經費需求說明

一、經費計算基準：人事費以各級人力人數、薪資估算；儀器設備費以單價及數量估算總價等。

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、**細部計畫** 1 前瞻資安技術研究(Security in Air & Security on Chip)	基礎研究	工程司	1. 發展國際共通性關鍵基礎設施防護規範。 2. 開發 IoT、5G 及 AI 等應用之資安工具。 3. 完成關鍵模組效能及旁通道攻擊之晶片驗證分析。 4. 培育關鍵資安技術研發人才與晶片資安研發人才。	1.每年開發 10 項相關之前瞻關鍵資安技術與機制，產學合作案 15 件，技轉 3 件，總金額達 600 萬以上。 2.每年培育高階資安技術研發人才 200 人次。 3.每年參與國	98,000	74,000	12,000	12,000	0	0	0

				際頂尖研討會發表論文8篇。							
二、**細部計畫** 2 雲端資安攻防平台(CDX)	基礎研究核心設施建置及維運	國家高速網路與計算中心	1. 完成 IoT、Bank Hacking 等產業場域研究。 2. 與企業合作辦理資安競賽，進行實證場域攻防演練。 3. 與產業進行產學合作，促進國內跨領域產業升級。	1. 每年辦理資安攻防演練1場。 2. 每年資安專業實務人才培訓90人次。 3. 每年提供450萬核心小時進行資安人才培育。 4. 每年進行國際間攻防平台發展趨勢與功能分析，撰寫技術報告1份。	27,000	8,500	7,000	9,000	0	2,500	0

經費分攤表(B008)

110 年度

跨部會 主提/申請機關 (含單位)	細部計畫名稱	負責內容	110 年度額度(千元)			
			一般科技施政	重點政策	前瞻基礎建設	申請數合計
各額度經費合計						

無經費分攤

111 年度

跨部會 主提/申請機關 (含單位)	細部計畫名稱	負責內容	111 年度額度(千元)			
			一般科技施政	重點政策	前瞻基礎建設	申請數合計
各額度經費合計						

無經費分攤

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	1								
110	2								
110	3								
總計									
111	1								
111	2								
111	3								
總計									

（主管機關名稱）

申購單價新臺幣 1000 萬元以上科學儀器送審表(B007)

中華民國 xxx 年度

申請機關(構)					
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	□申請機構作業基金(基金名稱：　　) □行政院國家科學技術發展基金(計畫名稱：　　) □政府科技預算(政府機關名稱：　　) □前瞻基礎建設特別預算(計畫名稱：　　) □其他(說明：　　)				
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：1000 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：_____

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

本計畫無此事項。

二、中程個案計畫自評檢核表(請以正本掃描上傳)

檢視項目	內　容　重　點 (內容是否依下列原則撰擬)	是
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)是否研提遴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	
	(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)經費自擔原則：	

檢視項目	內　容　重　點 (內容是否依下列原則撰擬)	是
	(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	
6.營運管理計畫	是否具務實及合理性(或能否落實營運)	V
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	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	
10.性別影響評估	是否填具性別影響評估檢視表	V
11.無障礙及通用設	是否考量無障礙環境，參考建築及活動空間相關規範辦	

檢視項目	內 容 重 點 (內容是否依下列原則撰擬)	是
	(3)是否檢附相關說明文件	
17.資通安全防護規劃	資訊系統是否辦理資通安全防護規劃	

主辦機關核章：承辦人 助理研究員(一)梁雁惠 單位主管 司長徐

主管部會核章：研考主管 會計主管

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：臺灣資安卓越深耕-學術型資安研究

主管機關（請填列中央二級主管機關）	科技部	**主辦機關（單位）**（請填列擬案機關／單位）	工程司

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）。	本計畫執行內容以技術研發及人才培育為主，並在計畫諮詢規劃會議中，安排女性專家學者參與，與性別平等政策綱領所強調消除性別隔離及營造性別友善工作環境、降低決策參與上的性別隔閡等重要議題相

	關。
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. 本專案屬國防資安領域，該領域學者群體於科技領域學者群體中偏少數，又該領域諮詢專家更為稀少，全台灣長年深耕於資訊安全領域之學者約為 40-50 位。 2. 本計畫在先期規劃諮詢專家包含 1 位女性參與及意見表達。未來專案執行團隊亦將具有女性成員。
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，	1. 本計畫在決審委員之組成，將會重視決審委員之性別組成。 2. 本案於未來推動時，就專家及研究團體進行性別統計，關注參與決策之性別平等及科技人才性別衡平性等性別議題。

宜關注不同性別可能未有平等取得社會資源之機會（例如:獲得政府補助；參加人才培訓活動），或平等參與社會及公共事務之機會（例如:參加公聽會/說明會）。 ②受益者受益程度之性別差距過大時（例如:滿意度、社會保險給付金額），宜關注弱勢性別之需求與處境（例如:家庭照顧責任使女性未能連續就業，影響年金領取額度）。 **c.公共空間** 公共空間之規劃與設計，宜關注不同性別、性傾向、性別特質及性別認同者之空間使用性、安全性及友善性。 ①使用性：兼顧不同生理差異所產生的不同需求。 ②安全性：消除空間死角、相關安全設施。 ③友善性：兼顧性別、性傾向或性別認同者之特殊使用需求。 **d.展覽、演出或傳播內容** 藝術展覽或演出作品、文化禮俗儀典與觀念、文物史料、訓練教材、政令/活動宣導等內容，宜注意是否避免複製性別刻板印象、有助建立弱勢性別在公共領域之可見性與主體性。 **e.研究類計畫** 研究類計畫之參與者（例如:研究團隊）性別落差過大時，宜關注不同性別參與機會、職場性別友善性不足等問題；若以「人」為研究對象，宜注意研究過程及結論與建議是否納入性別觀點。	
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）。	□有訂定性別目標者，請將性別目標、績效指標、衡量標準及目標值納入計畫書草案之計畫目標章節，並於本欄敘明計畫書草案之頁碼： ■未訂定性別目標者，請說明原因及確保落實性別平等事項之機制或方法。 1. 本計畫研究團隊之女性研究人員比例預計達 5%。 2. 本計畫諮詢、規劃及決審委

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。	員之女性委員，專家成員女性比例預計達 1/10。 3. 本案持續關注不同性別參與諮詢、規劃及決審階段之情形，以努力朝向任一性別比例不少於三分之一原則。
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。	■有訂定執行策略者，請將主要的執行策略納入計畫書草案之適當章節，並於本欄敘明計畫書草案之頁碼： 1. 本計畫之規劃諮詢人員包含 1 位女性，參與及意見表達。未來執行團隊亦將具有女性成員。 2. 本計畫未來在研究團隊的部分，將會鼓勵團隊積極培育女性研究人員，顧及女性研究人員參與的比例。 □未訂執行策略者，請說明原因及改善方法：

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

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

④ 培力弱勢性別，形成組織、取得發言權或領導地位。

d.培育專業人才

① 規劃人才培訓活動時，納入鼓勵或促進弱勢性別參加之措施

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

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

③ 培訓內涵中融入性別平等教育或宣導，提升相關領域從業人員之性別敏感度。

④ 辦理培訓活動之師資性別統計，作為未來師資邀請或師資培訓之參考。

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： 根據 2-2 本計畫所訂定之執行策略，僅在執行上鼓勵女性人員參與計畫的諮詢、規劃與執行，經費的編列上無調整。

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

參、評估結果

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

3-1 綜合說明	目前本計畫尚未開始對外徵求，仍在計畫內容規劃階段，然而，現階段已安排至少 1 位女性委員加入本計畫規劃諮詢委員，未來本計畫無論申請、審查、或執行將尊重不同性別，無限定性別皆可參與，並且將持續留意計畫未來人才培育之性別比例及女性委員參與會議的比例，以減少性別落差的情形。	
3-2 參採情形	3-2-1 說明採納意見後之計畫調整（請標註頁數）	1. 謝謝性別諮詢專家對於本計畫之肯定。 2. 據教育部統計處 107 年度統計資料顯示，女性大學畢業生在工程領域中所佔比例約 23%，且該領域女性研究人員的比例更偏低；除此之外，本計畫學術專長領域屬國防資安，108 年度資安領域計畫申請案僅佔資訊工程學門整體之 25%，並已有逐年下滑之趨勢，又於資安領域中女性申請比例僅佔 6.8%，目前本計畫先期規劃諮詢委員已安排 1 名女性委員參與，所佔比例約為 8.3%，本計畫將採納委員意見，先調高專家成員女性比例預計達 10%，女性人才培育比例至少 10%。
	3-2-2 說明未參採之理由或替代規劃	無

3-3 通知程序參與之專家學者本計畫之評估結果：

已於 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。

- **填表人姓名：梁雁惠 職稱：研究員 電話：02-27377525 填表日期：109 年 07 月 27 日**
- **本案已於計畫研擬初期□徵詢性別諮詢員之意見，或□提報各部會性別平等專案小組（會議日期：____年____月____日）**
- **性別諮詢員姓名：__服務單位及職稱：____ 身分：符合中長程個案計畫性別影響評估作業說明第三點第__1__款**（如提報各部會性別平等專案小組者，免填）

（請提醒性別諮詢員恪遵保密義務，未經部會同意不得逕自對外公開計畫草案）

【第二部分－程序參與】：由性別平等專家學者填寫

程序參與之性別平等專家學者應符合下列資格之一：

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

□2.現任或曾任行政院性別平等會民間委員。

□3.現任或曾任各部會性別平等專案小組民間委員。

（一）基本資料

1.程序參與期程或時間	109 年 07 月 23 日 至 109 年 07 月 25 日
2.參與者姓名、職稱、服務單位及其專長領域	林春鳳 屏東縣基督教女青年會 常務理事 休閒治療、休閒治動設計與帶領、性別主流化、體育行政
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	目前第一階段自評所敍述，諮詢委員僅有一位女性成員，佔全體之比例為何宜補充，其餘的統計資訊亦不明，建議補充可為參考之統計資料。
6.本計畫性別議題之合宜性	不同性別人才培育應被考慮在人才培育的議題中
7.性別目標之合宜性	目前訂定之性別目標為女性研究人才５%及女性參與決策比例為１／１０，因為不知現階段之統計資訊，無法判斷適宜性。
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	為國家資訊安全把關，長期建置我國在資訊不斷進步中的安全機制，人才培育也不斷新增數量，建議先了解目前不同性別在資訊領域之參與比例，或是在學習階段之不同性別比例，對於性別比例有明顯差異之情況應及時警覺並積極鼓勵有差異之性別成員參與並應用科學方法開發不同性

	別人才之潛能，以利我國在先進科技之競爭力。
（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）_____	

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
110-1901-04-20-05	臺灣資安卓越深耕-學術型資安研究	110	125,000	125,000	125,000	100%	
110-1901-04-20-05	臺灣資安卓越深耕-學術型資安研究	111	125,000	125,000	125,000	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	C2	學術型資安研究	125,000
2	111	C2	學術型資安研究	125,000
總計				250,000

備註：

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

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

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

2、 投入項目類別請用下列代號填寫：

2-1 系統開發

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

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

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

2-2 軟硬體採購

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

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

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

2-3 其他建議項目

(C1) 資安檢測標準研訂。

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

(C3) 新興資安領域之人才培育。

（C4） 編撰資安訓練教材。

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

五、其他補充資料

無。