政府科技發展中程個案計畫書

科技發展類前瞻基礎建設計畫

審議編號：114-5010-09-20-01

數位發展部資通安全署
「臺灣資安卓越深耕-資安卓越中心計畫(5/5)」
(核定本)

計畫全程：110 年 01 月至 114 年 8 月

中華民國 113 年 9 月

前後期別計畫內容修正對照表(A011)

前期(112 年-113 年)計畫名稱及經費審核情形：

前期(112 年-113 年)審查意見
1. 本計畫以「成為亞太高階資安人才及技術創新基地」為目標，設立資安卓越中心，推動項目包含資安 前瞻研究、頂尖實戰人才養成、實習場域建置等。本計畫為延續型計畫，綜觀 110 年度推動成果，本計畫推動目標及運作應屬可行。
2. 本計畫所擬定之關鍵成果與目標扣合度高，惟成果大多以操作型指標展現，不易評估其執行品質。建議本計畫增加執行效益於預期關鍵成果中，以利展現推動成果與亮點。特別是本計畫技術成果之“卓越”性，未能具體描述，應該於後續報告具體呈現與說明。
3. 本計畫宜有研發成果流向或串接之系統性規劃與運作，以利成果活化與反饋，加速政策目標之達成。 本計畫所研發之前瞻技術宜有技術研發或產業需求之 Benchmark，以印證所研發技術位居國際之領先群。
4. 因資安領域甚廣，本計畫年度推動時宜參考國際資安產業技術需求及中長期資安技術之發展，逐年進行研發議題微調，以確保前瞻資安技術之研發成果契合產業需求。本計畫之技術發展選題也應該考量以 中長期布局，讓行政院資安處「資安跨域整合聯防計畫」以短期、實務面布局，二計畫各自技術布局後則應建立對接機制，以利短、中、長期研究成果可落實到產業實務應用及整體政府防護。
5. 本計畫部分目標及關鍵成果已依初審意見完成修正，後續應經由各年度期中查核強化執行。
6. 本計畫所擬定之自我挑戰目標適切可行，惟本計畫須訂定資安人才品質之評估機制，以強化本計畫推 動人才培育之成效。另外提升之人才培育數及培訓學員數相對國內資安人才缺口，尚有一段差距，建議 本計畫加大人才培育之步調。
7. 本計畫需要與科技部學術型資安研究計畫搭配，提供研究資源及場域給學校作

人才培育用途，並且在國際交流與科技部的交流管道進行互補。於計畫報告上應提供具體合作成果。

8. 資安卓越中心預計於 112 年成立，隸屬於行政法人資安研究院，其人事費用將由行政法人編列預算支應。故本計畫執行過程中如完成前述行政法人成立，其編列之公務預算投入之同時應扣除本計畫所編列 之人事費用，避免重複編列。

序號	原計畫頁碼	前期(112 年-113 年)計畫內容（引原文或重點描述）	修正處頁碼	本期(114 年)計畫內容(引原文或重點描述)	修正原因
1	P.1 至 P.7	● 112-113 年之計畫目標、預期關建成果、經費及細部計畫等內容。 ● 前期(110-111 年)主要績效 ● 計畫連絡人	P.1 至 P.5	● 114 年之計畫目標、預期關建成果、經費及細部計畫內容。 ● 前期(112-113 年)主要績效 ● 計畫連絡人	配合第五期 114 年前瞻計畫，調整 114 年對應之項目內容，並更新計畫連絡人。
2	P.26	114 年完成技術轉移「累積」2 件及完成專利「累積」2 件	P.2、P.4 、P.16 、P.32 、P.43	114 年完成技術轉移「達」2 件及完成專利「達」2 件	配合委員審查意見，因該成果僅屬 114 年之目標值，故將「累積」2 件用詞一致改為「達」2 件，不影響工作指標。
3	P.20	表 3-1：工控場域建置規劃 112 年(發電及輸配電站)及 113-114 年(化工精煉場)建置場域為前期計畫規劃	P.24	表 3-1：工控場域建置規劃 更新 112 年(醫療)及 113-114 年(鐵道)建置場域	修正 112 年及 113-114 年工控場域建置項目及內容。
4	P.26 至 P.29	110 年之年度目標達成情形(重大效益)	P.17 至 P.20	新增 111 年至 112 年之年度目標達成情形(重大效益)	更新年度目標達成情形(重大效益)。

5	P.29 至 P.30	與以前年度差異說明(110 年至 111 年度與 112 年至 113 年度績效指標差異)	P.30 至 P.33	與以前年度差異說明(112 年至 113 年度與 114 年度績效指標差異)	更新與以前年度差異說明。
6	P.31 至 P.32	前期重要效益成果說明(110 年)	P.33 至 P.37	前期重要效益成果說明(110112 年)	更新前期重要效益成果說明。
7	P.34 至 P.36	工作指標(112 年至 113 年)及效益指標	P.38 至 P.39	工作指標(114 年)及效益指標	更新工作指標及效益指標
8	P.37	自我挑戰目標(112 年至 113 年)	P.40	自我挑戰目標(114 年)	補充 112 年至 113 年自我挑戰目標達成情形，並新增 114 年自我挑戰目標。
9	P.38 至 P.42	經費需求表(112-113 年)	P.41 至 P.43	經費需求表(114 年)	經費需求表更新為 114 年計畫之經費額度及內容。
10	P.15	無。	P.13 至 P.14	補充說明資安卓越中心成立之相關內容。	配合委員審查意見補充說明。

附表、前期(112 年-113 年)計畫細部經費配置

112 年

序號	細部計畫名稱	法定數(千元)	執行機構
1	臺灣資安卓越深耕-資安卓越中心計畫	320,000	國家資通安全研究院

113 年

序號	細部計畫名稱	法定數(千元)	執行機構
1	臺灣資安卓越深耕-資安卓越中心計畫	330,000	國家資通安全研究院

註：執行機構指受補助/委託之法人或學研單位(尚未執行可填「招標中」或「徵案中」)。

政府科技發展計畫書修正對照表(A009)

審議編號：114-5010-09-20-01

計畫名稱：臺灣資安卓越深耕-資安卓越中心計畫(5/5)

申請機關(單位)：數位發展部(資通安全署)

序號	審查意見	計畫修正說明	修正處頁碼
1	資安卓越中心是否成立	本計畫全程期間為 110 年 1 月 1 日至 114 年 8 月 31 日，110 年至 111 年原由國家實驗研究院執行，110 年即分別於臺北及臺南完成設置資安卓越中心辦公室。俟 112 年國家資通安全研究院(以下稱資安院)掛牌成立並承接執行本計畫後，資安卓越中心業務亦整併於資安院組織並持續運作中，有關資安卓越中心成立之詳細說明補充於計畫書 P.13-P.14。 另因應資安卓越中心已成立，相關文字亦配合調修，以避免混淆。	P.2 P13-P.14 P.36

附表、計畫目標及預期關鍵成果之修正對照表

項目	送審版	核定版	
經費	送審數 114 年：158,000 千元	核定數 114 年：158,000 千元	修正說明
計畫目標及預期關鍵成果	目標 1: 持續擴大工控場域攻防技術能量 關鍵成果 1:持續擴大攻防技術研發實驗室及攻防技術檢測實驗室能量，並用於國內高階實戰人才培育 關鍵成果 2 工控場域培訓高階學員達 15 人	目標 1: 持續擴大工控場域攻防技術能量 關鍵成果 1:持續擴大攻防技術研發實驗室及攻防技術檢測實驗室能量，並用於國內高階實戰人才培育 關鍵成果 2 工控場域培訓高階學員達 15 人	無修正
	目標 2: 推動本國資安高等研究成果落地 關鍵成果 1:頂尖研究團隊完成技術轉移達 2 件 關鍵成果 2:頂尖研究團隊完成專利達 2 件	目標 2: 推動本國資安高等研究成果落地 關鍵成果 1:頂尖研究團隊完成技術轉移達 2 件 關鍵成果 2:頂尖研究團隊完成專利達 2 件	無修正
	目標 3: 持續擴大國內頂尖實戰資安人才培訓能量 關鍵成果 1:邀請國外資安學界、業界和社群知名人士結合工控場域培訓國內及國際實戰人才至少 60 人	目標 3: 持續擴大國內頂尖實戰資安人才培訓能量 關鍵成果 1:邀請國外資安學界、業界和社群知名人士結合工控場域培訓國內及國際實戰人才至少 60 人	無修正

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

目 錄

壹、基本資料及概述表(A003)

<table>
<tr><td>審議編號</td><td colspan="4">114-5010-09-20-01</td></tr>
<tr><td>計畫名稱</td><td colspan="4">臺灣資安卓越深耕-資安卓越中心計畫</td></tr>
<tr><td>申請機關</td><td colspan="4">數位發展部</td></tr>
<tr><td>預定執行機關
(單位或機構)</td><td colspan="4">數位發展部資通安全署</td></tr>
<tr><td rowspan="3">預定
計畫主持人</td><td>姓名</td><td>謝翠娟</td><td>職稱</td><td>署長</td></tr>
<tr><td>服務機關</td><td colspan="3">數位發展部資通安全署</td></tr>
<tr><td>電話</td><td>(03)230-8954</td><td>電子郵件</td><td>tchsieh@acs.gov.tw</td></tr>
<tr><td>計畫摘要</td><td colspan="4">我國正值推動 DIGI+方案及 5+2 產業創新計畫，帶動產業數位升級，資安儼然已為最重要之基底，亟須培育充沛資安人才，本計畫以「成為亞太高階資安人才及技術創新基地」為目標，設立資安卓越中心，從資安前瞻研究、頂尖實戰人才養成、實習場域建置、國際合作及技術移轉創新育成等 5 個面向著手，挹注充足教學及研究資源，以厚植我國頂尖實戰人才培訓及資安前瞻研究能量，各面向重點內容如下：
1.前瞻研究：負責國家任務導向型研究，以提供政府機關短中期所需之應用技術研究為主，包括技術面及政策面等議題；另亦負責關鍵核心研究屬長期性基礎型研究，以發展國防、國安之關鍵技術及研究為主。
2.培育實戰頂尖人才：負責實戰型頂尖資安人才養成，擇優挑選產學政軍之人才進行培訓，完訓獲得較優渥之就業機會，並做為國家緊急需調用人力之後盾。
3.資安教學實習場域：建置國內關鍵基礎設施之工控場域，支援教育訓練及攻防演練之用，另於大學區網中心及政府開放場域，提供國內學研單位共享運用。
4.跨國合作：以資安卓越中心為對話窗口，與美洲、歐洲及澳洲等國外學術研究機構進行國際合作，包含進行跨國前瞻技術研究、參與國際組織進行資安標準制定、辦理大型國際學術會議發表研究成果等。
5.技術移轉及創新育成：透過技術移轉方式，幫助國內業者提升技術能力或成立新創公司，並運用經濟部、國發會、國科會等既有新創扶助資源，逐步壯大規模，站穩市場，進軍國際。</td></tr>
<tr><td rowspan="2">計畫目標、預期關鍵成果及與部會科技施政目標之關聯</td><td colspan="3">計畫目標及預期關鍵成果
114 年度</td><td>與部會科技施政目標之關聯</td></tr>
<tr><td colspan="3">目標 1: 持續擴大工控場域攻防技術能量
關鍵成果 1: 持續擴大攻防技術研發實驗室及攻防技術檢測實驗室能量，並用於國內高階實戰人才培育</td><td>深化數位應用，提升政府施政效能</td></tr>
</table>

	關鍵成果 2: 工控場域培訓高階學員達 15 人	
	目標 2: 推動本國資安高等研究成果落地 關鍵成果 1: 頂尖研究團隊完成技術轉移達 2 件 關鍵成果 2: 頂尖研究團隊完成專利達 2 件	深化數位應用，提升政府施政效能
	目標 3: 持續擴大國內頂尖實戰資安人才培訓能量 關鍵成果 1: 邀請國外資安學界、業界和社群知名人士結合工控場域培訓國內及國際實戰人才至少 60 人	深化數位應用，提升政府施政效能
預期效益	本計畫已成立資安卓越中心，目的在解決國內高階資安人才不足的問題，長期目標係成為亞太高階資安人才及技術創新基地，其功能包括資安前瞻研究、頂尖實戰人才養成、實習場域建置、國際合作交流、技術移轉創新育成等 5 項主要功能，預期效益重點說明如下： 1. 擇優挑選產學政軍之人才進行培訓，透過「以戰代訓」之理念，定期密集針對不同模擬場域進行實戰演練，提升學員實戰經驗，完訓獲得較優渥之就業機會，並做為國家緊急需調用人力之後盾，長期招收對象將擴及亞太地區。 2. 因應資安新興威脅及趨勢發展，由資安卓越中心延聘國際優秀人才，負責政府機關短中期所需之應用技術研究，以及國家長期關鍵核心之基礎研究，以培育並厚植我國資安前瞻研究自主能量；同時參與國際資安標準規範制定，確保開發技術與國際接軌，除可透過技轉方式，幫助國內業者提升技術能力或成立新創公司，亦可藉由資安前瞻研究成果進行國際合作，提升台灣國際能見度。 3. 於資安卓越中心建置國家型工控場域，提供國內關鍵基礎設施領域所需資安防護解決方案之實證場域，並支援教育訓練及大型攻防演練，另透過補助大學區網中心提供校園資安教學所需之場域設施，以及協調政府機關開放部份網路或應用系統供資安實習，拓展資安教學實習場域，完善資安教學設備環境。	
計畫群組及比重	請依群組比重填寫，需有比重最高之群組，且加總須 100%。 □ 生命科技 ____ %　□環境科技 ____ %　■數位科技 100 % □ 工程科技 ____ %　□人文社會 ____ %　□科技創新 ____ %	
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	
中長程個案計畫	■ 是，中長程個案計畫名稱：臺灣資安卓越深耕-資安卓越中心計畫	

<table>
<tr><td>資通訊建設計畫</td><td colspan="5">□ 是　　■ 否</td></tr>
<tr><td>政策依據</td><td colspan="5">1.PRESTSAIP-01090203040000：六大核心戰略產業推動方案：2.4 成立資安攻防機構，進行前瞻資安研究、國際合作
2.PRESTSAIP-01090204050000：六大核心戰略產業推動方案：2.5 成立資安攻防機構，進行人才培育
3.NSTP-20210101010000：國家科學技術發展計畫(民國 110 年至 113 年)：1-1-1.強化跨域育才彈性
4.CSIDAP-20180100000000：資安產業發展行動計畫(107-114 年)：一、建立需求導向之資安人才培訓體系
5.FIDP-20210206060000：前瞻基礎建設計畫(110 年修訂版)：4.6.6 臺灣資安越深耕-資安卓越中心計畫</td></tr>
<tr><td>計畫額度</td><td colspan="5">■ 前瞻基礎建設額度</td></tr>
<tr><td>執行期間</td><td colspan="5">114 年 01 月 01 日　至 114 年 8 月 31 日</td></tr>
<tr><td>全程期間</td><td colspan="5">110 年 01 月 01 日　至 114 年 8 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>113</td><td colspan="4">330,000</td></tr>
<tr><td rowspan="11">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">409,000</td></tr>
<tr><td>111</td><td colspan="4">400,000</td></tr>
<tr><td>112</td><td colspan="4">320,000</td></tr>
<tr><td>113</td><td colspan="4">330,000</td></tr>
<tr><td>114</td><td colspan="4">158,000</td></tr>
<tr><td>合計</td><td colspan="4">1,617,000</td></tr>
<tr><td rowspan="5">114 年度</td><td>人事費</td><td>0</td><td>土地建築</td><td>0</td></tr>
<tr><td>材料費</td><td>0</td><td>儀器設備</td><td>0</td></tr>
<tr><td>其他經常支出</td><td>126,400</td><td>其他資本支出</td><td>31,600</td></tr>
<tr><td>經常門小計</td><td>126,400</td><td>資本門小計</td><td>31,600</td></tr>
<tr><td colspan="2">經費小計(千元)</td><td colspan="2">158,000</td></tr>
<tr><td>部會施政計畫關鍵策略目標</td><td colspan="5">深化數位應用，提升政府施政效能</td></tr>
</table>

<table>
<tr><td>本計畫在機關施政項目之定位及功能</td><td colspan="4">1. 國家安全會議及行政院於 105 年 8 月共同召開「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；行政院據此於 106 年 11 月訂頒「國家資通安全發展方案(106 年至 109 年)」，期經前瞻政策引導及國家整體資源投入，逐步提升國家整體資安防禦能量。
2. 我國資通安全管理法於 108 年 1 月 1 日施行，目的為積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益。行政院資通安全處作為國家資通安全會報之幕僚單位，依資通安全管理法賦予之任務，持續推動資通安全專業人才之培育及資通安全產業之發展，並積極推動資通安全科技之研發、整合、應用、產學合作及國際交流合作，為我國資安生態系統注入更多活力。嗣為因應資安情勢嚴峻，於 109 年開始規劃「國家資通安全發展方案(110 年至 113 年)」。
3. 本計畫為主軸計畫，為發展數位應用資安生態系，完備 DIGI+及 5+2 產業創新方案資安能量，由行政院資通安全處橫向整合跨部會資源，成立資安卓越中心，定位為國家級前瞻研究中心，具備國際一流水準前瞻研究能量，從技術面及人才面為台灣未來 2030 資安需求扎根，目標成為亞洲地區代表性高階人才及技術創新基地。</td></tr>
<tr><td rowspan="5">計畫架構說明</td><td colspan="4">依細部計畫說明</td></tr>
<tr><td>細部計畫 1 名稱</td><td colspan="3">臺灣資安卓越深耕-資安卓越中心計畫</td></tr>
<tr><td>114 年度概估經費(千元)</td><td>158,000</td><td>計畫屬性</td><td>人才培育</td></tr>
<tr><td>主管機關</td><td>數位發展部</td><td>預定執行機構</td><td>數位發展部資通安全署</td></tr>
<tr><td>細部計畫重點描述</td><td colspan="3">1. 持續擴大工控場域攻防技術能量
2. 推動本國資安高等研究成果落地
3. 持續擴大國內頂尖實戰資安人才培訓能量</td></tr>
<tr><td>預期關鍵成果</td><td colspan="3">114 年預期關鍵成果：
1-1 持續擴大攻防技術研發實驗室及攻防技術檢測實驗室能量，並用於國內高階實戰人才培育
1-2 工控場域培訓高階學員達 15 人
2-1 頂尖研究團隊完成技術轉移達 2 件
2-2 頂尖研究團隊完成專利達 2 件
3-1 邀請國外資安學界、業界和社群知名人士結合工控場域培訓國內及國際實戰人才至少 60 人</td></tr>
</table>

<table>
<tr><td>前一年計畫或相關之前期程計畫名稱</td><td colspan="4">111-3601-09-20-01：臺灣資安卓越深耕-資安卓越中心計畫
112-5010-09-20-06：臺灣資安卓越深耕-資安卓越中心計畫(3/5)
113-5010-09-20-13：臺灣資安卓越深耕-資安卓越中心計畫(4/5)</td></tr>
<tr><td>前期
主要績效</td><td colspan="4">一、資安前瞻研究：完成期刊論文1篇(已投稿)、研討會論文5篇和技術論文3篇，共9篇論文報告。
二、頂尖實戰人才養成：
1. 開放工控資安之實戰課程訓練教材1套,內含 ICS 資安威脅趨勢與威脅、滲透測試實作、DMZ 攻防演練、內網滲透攻防演練、ICS 基礎與 PLC 程式設計、HMI 基礎程式實作、內網橫向擴散攻防演練、ICS 攻防演練等8門課程，以符合資安實務培訓所需。
2. 辦理資安菁英人才培訓課程，培訓具國際競爭力之資安實戰菁英人才，以政府單位資安技術人員、企業資安技術人員、資安公司研發人員為主，開設3期實務課程，計164人取得證書。
3. 組成國家資安聯隊 TWN48，參加2023世界駭客大賽(DEF CON)搶旗攻防賽(CTF)獲得全球第三名。
三、實習場域建置：
1. 臺北醫學大學偕同附屬醫院完成醫療場域建置，提供國內資安防護解決方案之實證場域，並支援教育訓練及攻防演練使用。同時舉辦工控資安實戰課程，受訓對象涵蓋產、政、軍及學等領域，計39位學員取得證書。
2. 完成政府骨幹網路實驗場域相關軟硬體及服務，萃取3個月政府骨幹實際流量做為實驗資料，供產學單位進行網路流量相關實驗驗測。
四、國際合作：完成對接國外頂級資安技術或研究機構共計5家，並與其中3家簽署合作備忘錄(立陶宛創新局、美加州大學柏克萊分校、德國馬克斯·普朗克安全與隱私研究所)，持續接軌國際資安發展及擴大合作。
五、技術移轉與創新育成：完成創新技術2項，並已被相關單位採用，已著手與有意願之單位簽署 MOU 並辦理後續技術移轉事宜。</td></tr>
<tr><td>跨部會署計畫</td><td colspan="4">□ 是 ■ 否</td></tr>
<tr><td>中英文關鍵詞</td><td colspan="4">資通安全、高階人才培育、前瞻研究、關鍵基礎設施場域、國際合作
Cyber Security, Talent Cultivation, Forward-Looking Research, Critical Infrastructure Testbed, International Cooperation</td></tr>
<tr><td rowspan="3">計畫連絡人</td><td>姓名</td><td>潘偉庭</td><td>職稱</td><td>分析師</td></tr>
<tr><td>服務機關</td><td colspan="3">數位發展部資通安全署</td></tr>
<tr><td>電話</td><td>(02)2380-8606</td><td>電子郵件</td><td>wt3180@acs.gov.tw</td></tr>
</table>

附錄 - 最終效益與各年度里程碑規劃表

最終效益(Endpoint)與里程碑(Milestone)規劃	修正說明
最終效益：成為亞太高階資安人才及技術創新基地。	
110 年度里程碑： 【年度目標】 1. 拓展資安教學實習場域，完善資安教學設備環境 2. 設立前瞻資安國際研究中心，提升本國資安高等研究能量 3. 建立實戰頂尖人才培訓機制，培訓國內頂尖實戰資安人才 【關鍵成果】 1-1 建置 1 個工控場域，培訓高階學員達 20 人 1-2 提升 GSN 骨幹網路惡意行為資料分析能量，並開放為高階研訓場域，現行 DNS 回溯能量由 3 個月提升至 1 年 1-3 建置 2 所區網中心成為資安高階教學實習場域，使用學員達 30 人 2-1 延攬國外高階研究人才，建立頂尖研究團隊，厚植我國資安前瞻研究自主能量，提出至少 9 篇研究報告、期刊論文、研討會論文或威脅情資報告 2-2 對接 1 家國外頂級資安技術或研究機構，接軌國際同時提升台灣資安研發之能見度 3-1 建立 1 套頂尖資安實戰課程及培訓機制，並用於國內高階實戰人才培育 3-2 邀請國內資安國際競賽得獎團隊培訓國內高階實戰人才至少50人	

最終效益(Endpoint)與里程碑(Milestone)規劃	修正說明
111 年度里程碑： 【年度目標】 1. 持續擴充工控場域，並建置政府開放場域基礎環境 2. 持續提升本國資安高等研究能量 3. 完善自主實戰頂尖人才培訓機制，培訓國內頂尖實戰資安人才 【關鍵成果】 1-1 持續建置工控場域累積達 2 個，並設置攻防實戰教室，培訓高階學員達 30 人 1-2 建置政府開放場域主要機房與資安實習實驗室，作為政府資安專責人員培訓場域 1-3 建立政府開放場域營運制度，作為政府資安專責人員培訓場域 2-1 持續延攬國外高階研究人才，擴大頂尖研究團隊規模，厚植我國資安前瞻研究自主能量，提出至少 9 篇研究報告、期刊論文、研討會論文或威脅情資報告 2-2 對接國外頂級資安技術或研究機構累積達 2 家，持續接軌國際同時提升台灣資安研發之能見度 3-1 完善建立自主頂尖資安實戰課程，並用於國內高階實戰人才培育 3-2 邀請國外資安學界、業界和社群知名人士培訓國內實戰人才至少 50 人	

最終效益(Endpoint)與里程碑(Milestone)規劃	修正說明
112 年度里程碑： 【年度目標】 1. 持續擴充工控場域，並開放政府場域資料供產學研究 2. 擴大本國資安高等研究能量，並辦理國際大型資安學術或技術會議 3. 結合工控場域建置，開發相關實戰訓練教材 【關鍵成果】 1-1 持續建置工控場域累積達 3 個，並設置攻防技術研發實驗室，培訓高階學員達 30 人 1-2 建置威脅情資加值分析/索引系統，開放 3 個月政府骨幹網路 Meta data 資料量，供產學研究 2-1 持續延攬國外高階研究人才，擴大頂尖研究團隊規模，厚植我國資安前瞻研究自主能量，提出至少 9 篇研究報告、期刊論文、研討會論文或威脅情資報告 2-2 對接國外頂級資安技術或研究機構累積達 3 家，持續接軌國際同時提升台灣資安研發之能見度 2-3 辦理 1 場大型國際資安學術或技術會議，參與人數至少 200 人 3-1 邀請國外資安學界、業界和社群知名人士結合工控場域培訓國內實戰人才至少 125 人 3-2 結合工控場域建置與開發 1 套資安實戰訓練教材	

最終效益(Endpoint)與里程碑(Milestone)規劃	修正說明
113 年度里程碑： 【年度目標】 1. 持續擴充工控場域，並擴充政府開放場域環境實驗能量 2. 持續擴大本國資安高等研究能量 3. 自主開發國際化培訓教材，並招收國際培訓學員 【關鍵成果】 1-1 持續建置工控場域累積達 4 個，並設置攻防技術檢測實驗室，培訓高階學員達 30 人 1-2 建置可模擬機關網路環境與應用系統之實驗場域，並擴增開放政府骨幹網路 Meta data 資料量 2-1 持續延攬國外高階研究人才，擴大頂尖研究團隊規模，厚植我國資安前瞻研究自主能量，提出至少 9 篇研究報告、期刊論文、研討會論文或威脅情資報告 2-2 對接國外頂級資安技術或研究機構累積達 4 家，持續接軌國際同時提升台灣資安研發之能見度 3-1 完成自主頂尖資安實戰課程國際化，並開始對國際招生，至少招收國際學生 20 人 3-2 邀請國外資安學界、業界和社群知名人士結合工控場域培訓國內及國際實戰人才至少 125 人	

最終效益(Endpoint)與里程碑(Milestone)規劃	修正說明
114 年度(8 月)里程碑： 【年度目標】 1. 持續擴大工控場域攻防技術能量 2. 推動本國資安高等研究成果落地 3. 持續擴大國內頂尖實戰資安人才培訓能量 【關鍵成果】 1-1 持續擴大攻防技術研發實驗室及攻防技術檢測實驗室能量，並用於國內高階實戰人才培育 1-2 工控場域培訓高階學員達 15 人 2-1 頂尖研究團隊完成技術轉移至少 2 件 2-2 頂尖研究團隊完成專利至少 2 件 3-1 邀請國外資安學界、業界和社群知名人士結合工控場域培訓國內及國際實戰人才至少 60 人	

貳、計畫緣起

一、政策依據

為因應國家發展之資安人力需求，行政院訂頒「第五期國家資通安全發展方案(106 年至 109 年)」及「資安產業發展行動計畫(107-114年)」，由行政院資通安全處、教育部、國科會及經濟部等機關(單位)推動辦理，並以厚植資安專業人才為實施重點，推動相關計畫挹注資源布建資安培育環境，強調以實務與產學鏈結為導向之創新培育模式，結合國內大學校院資安教學能量，期建立以需求為導向之資安人才培訓體系為目標，孕育優質資安人才，提供我國各產業所用，已建立培訓能量，我國資安人才培育現況如圖 2-1 所示。

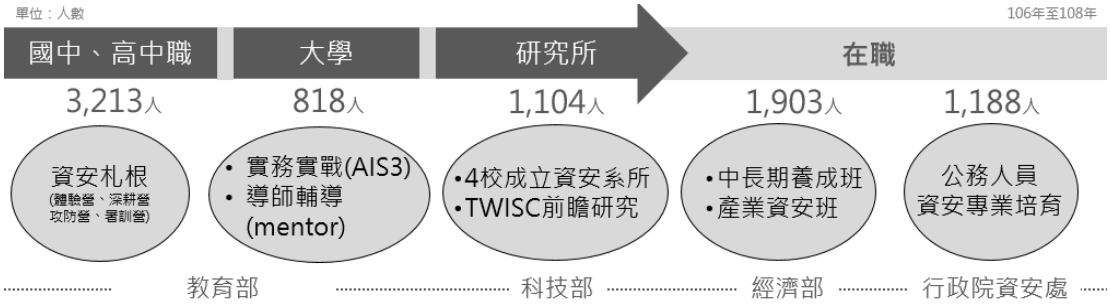

圖 2-1：我國資安人才培育現況

我國正值推動 DIGI+方案及 5+2 產業創新計畫，帶動產業數位升級，資安儼然已為最重要之基底(如圖 2-2)，亟須培育充沛資安人才，以全面強化產業及政府機關資安防護量能。

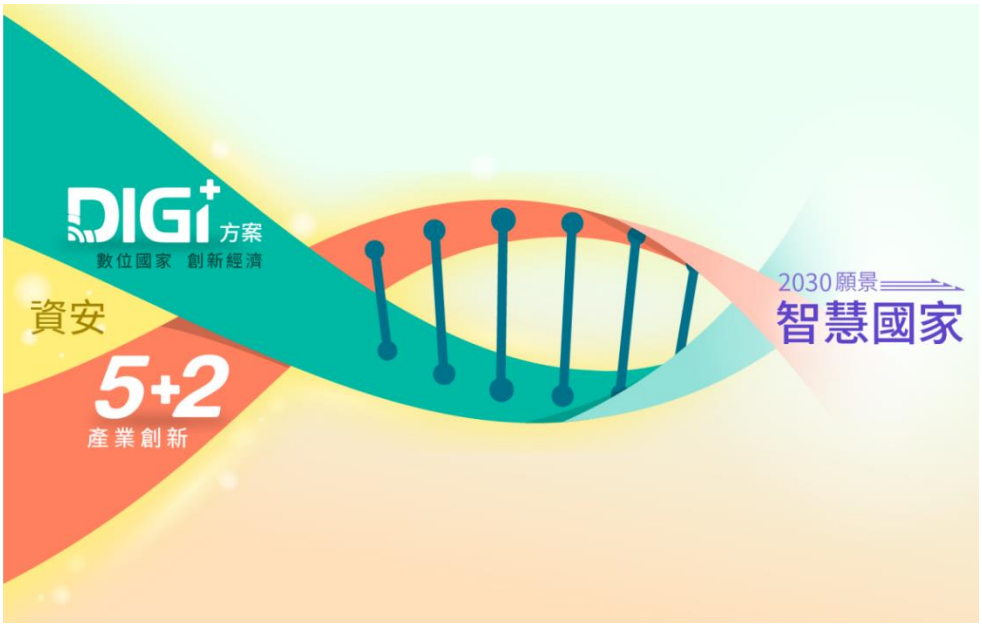

圖 2-2：資安為基底推動產業發展以邁向智慧國家

二、目前環境需求分析與未來環境預測說明

隨著數位經濟快速發展，致資安威脅程度亦加劇，使政府和產業對於資安防護及研發人才需求大增，凸顯現有資安人培質量的不足，經行政院資通安全處盤點目前現況：

1、校園部分：已推動 4 所大專院校自 108 年起成立 5 個資安碩士(學程)班，逐步建置系統性資安人才培育體系，惟目前仍欠缺師資員額及教學資源。

2、產業部分：經濟部針對待業者開設中長期養成班，企業在職員工開設產業資安班，關鍵基礎設施開設金融、物聯網及工控等資安課程，106 至 108 年累計培訓 1,903 名資安人才，培訓內容包含系統滲透測試攻防、資安事件鑑識、資安攻防與監控、Web 應用滲透測試、無線網路與物聯網安全、關鍵基礎設施資安攻擊與防護等資安課程。其中，107 至 108 年中長期養成班完訓學員計有 124 人，成功媒合就業者達 81 人；另，經濟部透過結合產業人才能力鑑定機制(iPAS)，107 年起建立 iPAS 資安工程師初級鑑定認證，108 年新增中級鑑定認證，接軌資安產業用人需求，iPAS 資訊安全工程師能力鑑定累計 3,021 人次報考；惟產業各界多次反應仍缺乏實戰人才及跨域人才。

3、國家部分：我國自 90 年開始，每 4 年訂頒國家資通安全發展方案，以推動資通安全基礎建設工作，迄今已完成諸多階段性里程碑，包括國家整體資安聯防機制、政府機關資安防護能量、網路犯罪偵防技術、資安產業發展推動等，惟就資安前瞻研究部分，目前仍學研機構為主，有關高等研究能量則較缺乏國家整體發展之策略及成果。

為解決資安專業人才及跨域人才短缺之問題，其策略建議應先從儘速補實資安師資員額短缺著手，並挹注充足教學及研究資源，以培育具實戰經驗頂尖人才及前瞻研究人才，如圖 2-3 所示。

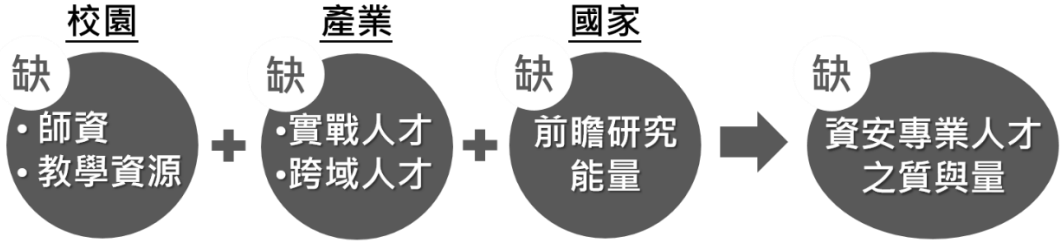

圖 2-3：資安人才盤點現況

行政院資通安全處參考各界所提政策建言，據以研提資安人才卓越計畫(草案)，規劃長期資安人才培育目標與策略(如圖 2-4)。

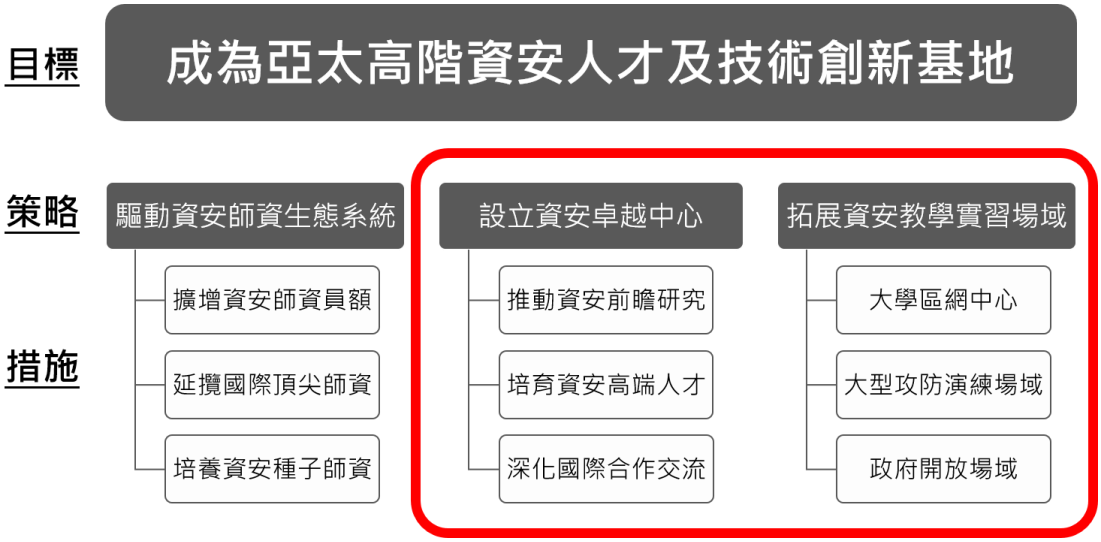

圖 2-4：長期資安人才培育目標與策略

三、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

本計畫為主軸計畫，依據資安人才卓越計畫之「設立資安卓越中心」及「拓展資安教學實習場域」等策略研提，為發展數位應用資安生態系，完備 DIGI+及 5+2 產業創新方案資安能量，由行政院資通安全處橫向整合跨部會資源，成立資安卓越中心，定位為國家級前瞻研究中心，具備國際一流水準前瞻研究能量，從技術面及人才面為台灣未來 2030 資安需求扎根，目標成為亞洲地區代表性高階人才及技術創新基地，分從資安前瞻研究、頂尖實戰人才養成、實習場域建置、國際合作及技術移轉創新育成等 5 個面向著手，挹注充足教學及研究資源，以厚植我國頂尖實戰人才培訓及資安前瞻研究能量。

本計畫全程期間為 110 年 1 月 1 日至 114 年 8 月 31 日，計畫初期(110-111 年)由財團法人國家實驗研究院(以下簡稱國研院)、前行政院資通安全會報技服中心(以下簡稱技術服務中心)及教育部等 3 個單位分工辦理，110 年國研院於臺南沙崙資安暨智慧科技研發大樓設置「資安卓越中心」臺南辦公室，於 110 年 10 月上旬已有研究人員進駐；另與臺北科技大學合作假先鋒國際研發大樓設置「資安卓越中心」臺北辦公室，並於 110 年 12 月 27 日進行啟用儀式。

俟 112 年 2 月 10 日國家資通安全研究院(以下簡稱資安院)掛牌成立並承接執行本計畫，資安卓越中心亦整併於資安院組織架構並持續運作中。資安院業務囊括前技術服務中心與資安卓越中心之範疇，主要為研發資通安全科技，推動資通安全技術應用、移轉、產學服務及國

際合作交流，除在原有基礎上持續努力外，而由多單位合作轉型為集中管理，亦可帶來高效資源利用與專注資安研究發展。

參、計畫目標與執行方法

一、目標說明

計畫全程總目標(end point)					
成為亞太高階資安人才及技術創新基地					
里程碑(milestone)					
年度	第一年 民 110 年	第二年 民 111 年	第三年 民 112 年	第四年 民 113 年	第四年 民 114 年 (8 月)
年度目標	1. 拓展資安教學實習場域，完善資安教學設備環境 2. 設立前瞻資安國際研究中心，提升本國資安高等研究能量 3. 建立實戰頂尖人才培訓機制，培訓國內頂尖實戰資安人才	1. 持續擴充工控場域，並建置政府開放場域基礎環境 2. 持續提升本國資安高等研究能量 3. 完善自主實戰頂尖人才培訓機制，培訓國內頂尖實戰資安人才	1. 持續擴充工控場域，並開放政府場域資料供產學研究 2. 擴大本國資安高等研究能量，並辦理國際大型學術會議 3. 結合工控場域建置，開發相關實戰訓練教材	1. 持續擴充工控場域，並擴充政府開放場域環境實驗能量 2. 持續擴大本國資安高等研究能量 3. 自主開發國際化培訓教材，並招收國際培訓學員	1. 持續擴大工控場域攻防技術能量 2. 推動本國資安高等研究成果落地 3. 持續擴大國內頂尖實戰資安人才培訓能量
預期關鍵成果	1-1. 建置 1 個工控場域，培訓高階學員達 20 人 1-2. 提升 GSN 骨幹網路惡意行為資料分析能量，並開放為高階研訓場域，現行 DNS 回溯能量由 3 個月提升至 1 年 1-3. 建置 2 所區網中心成為資安高	1-1. 持續建置工控場域累積達 2 個，並設置攻防實戰教室，培訓高階學員達 30 人 1-2. 建置政府開放場域主要機房與資安實習實驗室，作為政府資安專責人員培訓場域 1-3. 建立政府	1-1. 持續建置工控場域累積達 3 個，並設置攻防技術研發實驗室，培訓高階學員達 30 人 1-2. 建置威脅情資加值分析/索引系統，開放 3 個月政府骨幹網路 Meta data 資料量，供產學研究	1-1. 持續建置工控場域累積達 4 個，並設置攻防技術檢測實驗室，培訓高階學員達 30 人 1-2. 建置可模擬機關網路環境與應用系統之實驗場域，並擴增開放政府骨幹網路 Meta data	1-1. 持續擴大攻防技術研發實驗室及攻防技術檢測實驗室能量，並用於國內高階實戰人才培育 1-2. 工控場域培訓高階學員達 15 人 2-1. 頂尖研究團隊完成技術轉移

	階教學實習場域，使用學員達30人 2-1. 延攬國外高階研究人才，建立頂尖研究團隊，厚植我國資安前瞻研究自主能量，提出至少9篇研究報告、期刊論文、研討會論文或威脅情資報告 2-2. 對接1家國外頂級資安技術或研究機構，接軌國際同時提升台灣資安研發之能見度 3-1. 建立1套頂尖資安實戰課程及培訓機制，並用於國內高階實戰人才培育 3-2. 邀請國內資安國際競賽得獎團隊培訓國內高階實戰人才至少50人	開放場域營運制度，作為政府資安專責人員培訓場域 2-1. 持續延攬國外高階研究人才，擴大頂尖研究團隊規模，厚植我國資安前瞻研究自主能量，提出至少9篇研究報告、期刊論文、研討會論文或威脅情資報告 2-2. 對接國外頂級資安技術或研究機構累積達2家，持續接軌國際同時提升台灣資安研發之能見度 3-1. 完善自主頂尖資安實戰課程，並用於國內高階實戰人才培育 3-2. 邀請國外資安學界、業界和社群知名人	2-1. 持續延攬國外高階研究人才，擴大頂尖研究團隊規模，厚植我國資安前瞻研究自主能量，提出至少9篇研究報告、期刊論文、研討會論文或威脅情資報告 2-2. 對接國外頂級資安技術或研究機構累積達3家，持續接軌國際同時提升台灣資安研發之能見度 2-3. 辦理1場大型國際資安學術或技術會議，參與人數至少200人 3-1. 邀請國外資安學界、業界和社群知名人士結合工控場域培訓國內實戰人才至少125人 3-2. 結合工控場域建置	資料量 2-1. 持續延攬國外高階研究人才，擴大頂尖研究團隊規模，厚植我國資安前瞻研究自主能量，提出至少9篇研究報告、期刊論文、研討會論文或威脅情資報告 2-2. 對接國外頂級資安技術或研究機構累積達4家，持續接軌國際同時提升台灣資安研發之能見度 3-1. 完成自主頂尖資安實戰課程國際化，並開始對國際招生，至少招收國際學生20人 3-2. 邀請國外資安學界、業界和社群知名人士結合工控場域培訓國內及	達2件 2-2. 頂尖研究團隊完成專利達2件 3-1. 邀請國外資安學界、業界和社群知名人士結合工控場域培訓國內及國際實戰人才至少60人

		士培訓國內實戰人才至少 50 人	與開發1套資安實戰訓練教材	國際實戰人才至少 125 人	
年度目標達成情形(重大效益)	1. 資安前瞻研究：完成資安威脅情資報告12篇、期刊論文9篇、研討會論文4篇、技術論文(尚未發表)7篇、產業研究政策報告5篇、4套後量子密碼自動化驗證工具、6個同態加密技術、1個社群網路資料平台及提供威脅情資平台服務。 2. 頂尖實戰人才養成：建立1套共36門資安培訓模組化課程(含7門管制課程)，並辦理資安菁英班與網路威脅防禦競賽，共培訓55名學員，51名通過評測，並建置以藍軍為主的紅藍攻防平台供競賽及訓練使用。 3. 實習場域建置：以中油大林煉油廠之煉油訓練實	1. 資安前瞻研究：完成威脅情資報告28篇、國家任務導向型報告5篇、研討會論文4篇、技術論文(尚未發表)16篇、CVE漏洞挖掘揭露報告12篇、惡意程式分析平台、更新「社群網路資料平台」為「網路社群分析平台」、異常資訊分析平台、深度偽造影音分析平台、網路大數據資料庫、維運威脅情資平台。 2. 頂尖實戰人才養成： (1) 完成紅藍攻防平台腳本3套、完成資安課程擴充13類主題，共64門課程。 (2) 完成高階實戰人才培訓通過84人、國家級資安戰隊成員已	1. 資安前瞻研究：完成期刊論文1篇(已投稿)、研討會論文5篇和技術論文3篇，共9篇論文報告。 2. 頂尖實戰人才養成： (1) 開放工控資安之實戰課程訓練教材1套，內含ICS 資安威脅趨勢與威脅、滲透測試實作、DMZ 攻防演練、內網滲透攻防演練、ICS基礎與 PLC 程式設計、HMI 基礎程式實作、內網橫向擴散攻防演練、ICS攻防演練等8門課程，以符合資安實務培訓所需。 (2) 辦理資安菁英人才培訓課程，培訓具國際競爭力		

	習場域做為OT場域，搭配技服中心自建IT虛擬場域，將OT場域與IT場域整合，模擬能源領域之真實環境，並以此虛擬場域培訓21名學員；另為提供校園資安教學所需之場域設施，以已設立之區網中心為實習場域融入教學實習並進行實作驗證，於臺北區網中心規劃建置區網封包蒐集系統，桃竹苗區網中心開設EC-Council Certified Ethical Hacker (CEH)駭客技術專家認證課程，共有32名學員完成培訓；為以政府骨幹網路為基礎，發展網路流量與威脅分析技術，以供學員實務分析與學習使用，將政府骨幹網路基礎頻寬架構	培訓55人。 (3) 完成高階學員工控資安實戰課程培訓，本課程受訓對象涵蓋產、政、軍及學等領域，共計30人。 (4) 辦理國際資安講座，參與人數18人。 3. 實習場域建置： (1) 完成台水公司新營員工訓練園區水資源工控模擬場域建置，參考台水公司現有網路架構環境，整合IT場域與OT場域，並透過演練平台即時呈現演練過程。 (2) 完成政府開放場域機房與資安實習實驗室建置，提供場域供產學研單位進行相關資安研析與驗證。	之資安實戰菁英人才，以政府單位資安技術人員、企業資安技術人員、資安公司研發人員為主，開設3期實務課程，計164人取得證書。 (3) 組成國家資安聯隊TWN48，參加2023世界駭客大賽（DEF CON）搶旗攻防賽(CTF)獲得全球第三名。 3. 實習場域建置： (1) 臺北醫學大學偕同附屬醫院完成醫療場域建置，提供國內資安防護解決方案之實證場域，並支援教育訓練及攻防演練使用。同時舉辦工控資安實戰課程，受訓對象涵		

	提升至100G，擴充介接能量至100G 流量。 4. 國際合作：與加州大學柏克萊分校長期網路安全研究中心(Center for Long-Term Cybersecurity, CLTC) 簽訂合作意向書。 5. 技術移轉與創新育成：完成技術移轉與創新育成評估報告2篇，並舉辦產業座談會。	(3) 於臺大、陽明交大之區網中心各建置1個資安教學實習場域，於臺大完成區網封包蒐集與鑑識系統及資安大數據分析平臺建置，並開辦 30 小時資安大數據分析課程；於陽明交大開設40小時 EC-Council Certified Ethical Hacker (CEH) 駭客技術專家認證課程，共20名通過證照考試。 4. 國際合作： (1) 與德國馬克斯普朗克安全及隱私研究所 (MPI-SP) 簽訂 MoU。 (2) 與日本情報通信研究機構 (NICT) 簽訂 MoU(輪簽階段)，並向 NICT 展示	蓋產、政、軍及學等領域，計39位學員取得證書。 (2) 完成政府骨幹網路實驗場域相關軟硬體及服務，萃取3個月政府骨幹實際流量做為實驗資料，供產學單位進行網路流量相關實驗驗測。 4. 國際合作： (1) 完成對接國外頂級資安技術或研究機構共計5家，並與其中3家簽署合作備忘錄(立陶宛創新局、美加州大學柏克萊分校、德國馬克斯·普朗克安全與隱私研究所)，持續接軌國際資安發展及擴大合作。 (2) 與日本情報通信研究機構 (NICT)、資		

		以藍軍為主的攻防平台，此外邀請日本NICT與SecHack365校友參與資安防禦競賽。 (3) 辦理2022年第12屆量子密碼學國際會議。 5. 技術移轉與創新育成：完成產業評估報告3篇，並舉辦2場產業座談會及3場產業交流會。	通安全研究與教學中心、國科會臺灣資安科技研究中心共同辦理「2023 TWN-NICT Cybersecurity Workshop」，並邀請NICT與SecHack365校友參與網路威脅防禦競賽。 5. 技術移轉與創新育成：完成創新技術2項，並已被相關單位採用，已著手與有意願之單位簽署MOU並辦理後續技術移轉事宜。		

二、執行策略及方法

本計畫架構與執行包含資安前瞻研究、頂尖實戰人才養成、實習場域建置、國際合作交流、技術移轉創新育成等五個分項(計畫架構如圖 3-1)，以下將對各分項細部說明：

圖 3-1：本計畫架構

(一)資安前瞻研究

資安卓越中心定位為國家級前瞻資安國際研究中心(類似國家衛生研究院)，主管此機構之政府機關層級將具一定之高度，未來此研究中心將朝固定經費挹注以支持其永續運作之方向努力，並將主動出擊，積極網羅海外人才，以延攬頂尖高階研究人員及打造一流培訓師資團隊作為追求卓越之第一要務。為確保此研究中心之長期研究績效，將參考美國國家型實驗室或研究機構，設計完善之行政與技術等監督機制。

此研究中心之研究議題多屬機敏，參與此研究中心之研究學者應進行安全查核(視議題敏感程度予以分級)，並規劃以專任方式聘用，有效保護研究成果。但屬於學術研究議題者可以採用開放原碼(open source)並於國際資安研究社群會議發表，以建立國際聲譽與國際合作網絡。

本分項以「國家任務導向研究」、「關鍵核心研究」兩大主軸，其關鍵細部說明如下：

1. 國家任務導向型研究

以提供政府機關短中期所需之應用技術研究為主，包括技術面(如主動式防禦技術、惡意攻擊溯源追蹤、弱點挖掘自動化、駐外館處之安全網路通訊技術、5G 政府網路之資安防護架構等)及政策面(如跨國網路戰之國際法規研究、平戰轉

移等)議題。每一年度研究主題將定期邀請產、官、學、研界專家召開會議，視當前資安政策需求訂定研究方向與主題。

2. 關鍵核心研究

屬長期性基礎型研究，以發展國防、國安之關鍵技術及研究為主，如量子與後量子密碼技術，人工智慧資安攻防技術、暗網攻防技術、零時差弱點研究及解決方案(含工控系統)等。但具機敏性質之研究成果仍將建立其績效查證機制，以維持此研究中心之資源投入效率。

關鍵核心研究將聚焦於下列三項主軸：

(1) 網路威脅防禦：發掘潛在網路威脅，增進抵禦威脅能力，提升國家資安體質。例如建立我國網路威脅資料庫、國內慣用系統(如公文系統)弱點偵測、防護與修補工具等。同時維續威脅情報平台，提供威脅情資供資安學者進行查詢，每月針對國際重大資安事件定期發布技術報告及高危惡意程式樣本。

(2) 網路數據分析：關注分析網路數據，偵測應對異常資訊，打造安全網路空間。例如異常資訊內容偵測於社交工程識別、應用異常資訊流量偵測於深度造假識別、深度造假識別應用於異常資訊內容偵測、深度造假的社交工程攻擊之偵測與防護技術、新型態之數位鑑識技術等。

(3) 先進密碼研究：強化先進密碼架構，因應電腦算力提升，確保網路加密安全。例如先進密碼演算法研究、先進密碼演算法應用套件開發、先進加密安全晶片實作等。

資安卓越中心研究人力負責前揭各項研究，研究人力來源規劃以專任為主、兼任為輔之方式，將延攬國內外知名或年輕具潛力之資安學者及技術專家回國。考量此研究中心之研究議題多屬機敏性，未來將朝設自有之運算基礎設施之方向進行規劃，但將視研究性質之機敏性質一部分兼用使用外部運算設施以減省經費。

(二)頂尖實戰人才養成

目前政府與產業界均存在攻與防之資安人才需求，而高階之攻防

人才養成不易，除須具備資訊及資安之基本知識與技能外，尚須多年實務經驗之累積與技術之鑽研，始能成為高階人才，而此揭人才從國內外經驗來看，即具投入新創之潛能，爰本計畫所訓練之人才，將以高階之資安攻防實務、密碼學及破密分析、數位鑑識實務、系統漏洞分析及挖掘、資安威脅情資整合應用等為主，並持續蒐集產政學研專家意見後調整，另人才的分級鑑定，也是本中心任務，未來將發展人才鑑定與證照制度，俾利做為產業用人參考。本分項細部說明如下：

1. 培訓對象

初期培訓對象聚焦我國具資安潛力菁英，擇優挑選產學政軍之人才進行培訓，施予訓練計畫，在相當學、經歷等客觀條件下，優先調訓女性，以減少資通訊領域職業性別隔離情形。並針對不同類型資安人才，規劃不同評核機制(如取得相關證照或通過考試等)，完訓之頂尖人才獲得較優渥之就業機會，並可協助政府及關鍵資訊基礎設施(CII)資安防護，做為國家緊急需調用人力之後盾，長期招收對象將擴及亞太地區，並以成為亞太資安頂尖人才培育基地為目標，架構如圖 3-2。

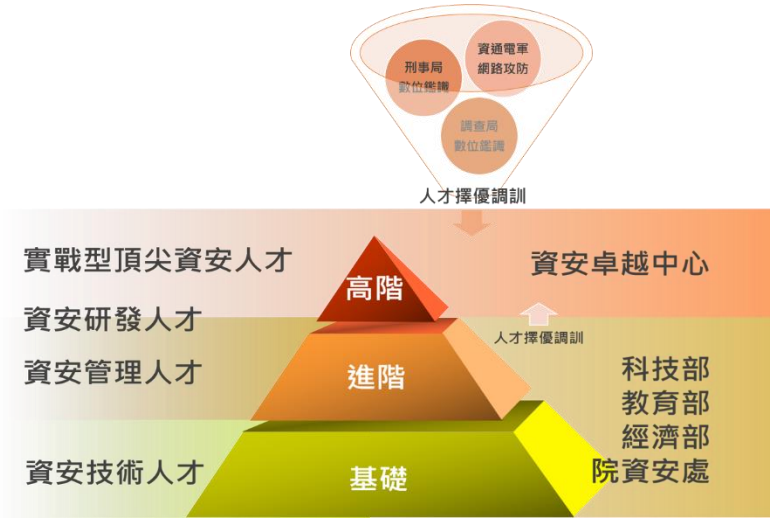

圖 3-2：實戰型頂尖資安人才養成架構

2. 師資來源

以優於教授級專業技術人員薪資水準聘請擔任講師，邀請國內外一流資安競賽團隊、業師、學界和社群知名人士，如 SANS 講師，以個人實戰經驗及實務操作之方式，講授完整資安白帽駭客實戰技術培訓課程。

3. 培訓教材

初期參考國外頂尖資安課程，如 SANS NetWars，議題涵蓋 Web Security、Mobile Security、Linux 系統安全、Reverse engineering 解析、SCADA Security、Digital Forensic 實戰等資安關鍵技術；中期逐步結合工控場域建置，開發自主實戰訓練教材；長期以自主開發國際化培訓教材為目標。

實戰型頂尖資安人才養成將搭配工控場域建置(示意圖如圖 3-3)，設置攻防實戰教室、攻防技術研發實驗室、攻防技術檢測實驗室，透過「以戰代訓」之理念，定期密集針對不同模擬場域進行實戰演練，提升學員實戰經驗。

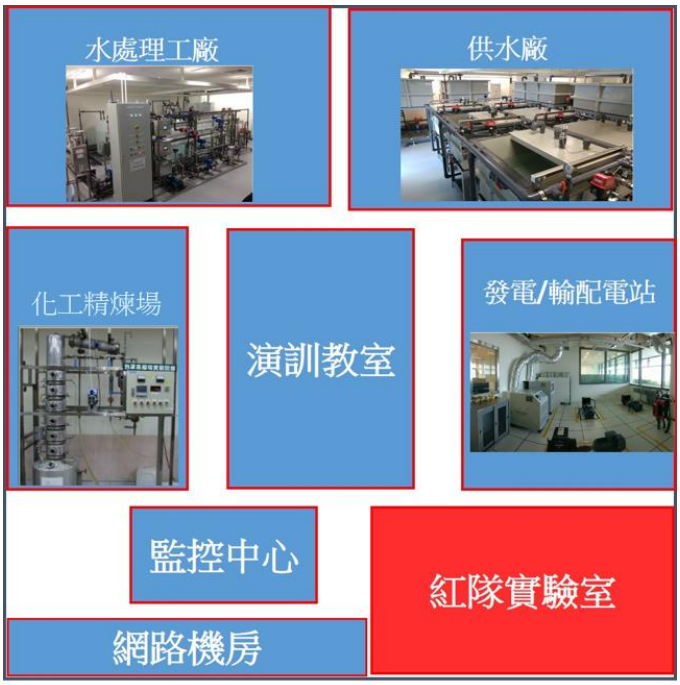

圖 3-3：工控場域建置示意圖

(三)實習場域建置：

為完善資安教學設備環境，由資安卓越中心監督並協調規劃各種實習、實驗、實測及實戰場域，拓展資安教學實習環境，提供頂尖資安人才培育資源。本分項以「工控場域」、「大學區網中心」及「政府開放場域」三大主軸(如圖 3-4)，其關鍵細部說明如下：

圖 3-4：實習場域建置規劃

1. 工控場域

資安卓越中心將定期評估國內各關鍵基礎設施人才需求之迫切性、需求量及優先順序等，進行國家型工控/OT 場域之整體性規劃。自 110 年至 113 年間，每年建置一座國內關鍵基礎設施之工控場域於資安卓越中心(初步規劃如表 3-1，後續將每年定期評估，並視結果滾動調整)，包括能源、水資源、衛生醫療、交通等各領域，主要用以支援教育訓練及攻防演練。

表 3-1：工控場域建置規劃

年度 / 規劃內容	110年度	111年度	112年度	113-114年度
建置項目	煉油廠	水處理工廠	醫療模擬場域	鐵道模擬場域(暫定)
需求空間	以網路連線OT與處擬IT場域	60坪	10坪	20坪
工廠情境	進行原油蒸餾、分離與精煉，並儲存及運送成品	從取得原水、然後進行投孳及過濾、再至加氯消毒，最後供水	癌症化療病房，給藥系統分派指定藥物給與病人，護理人員設定輸液幫浦相關參相關參數，以定時定量提病患進行藥物注射	以鐵道號誌系統為基礎，模擬轉轍器、平交道、號誌機等聯鎖設備運作邏輯，並整合號誌軟體
控制系統	● ENG ● HIS ● OP ● PLC	● SCDA ● PLC	● HIS ● NIS	● SCADA

為提升國內關鍵基礎設施資安防護能量，依照廠區實際作業流程及操作環境，比照實際廠區樣態建置工控實驗測試場域，達到防護網路實體系統(Cyber Physical Systems)如

水處理、供水、發電及輸配電及石化天然氣等流程，並且進行從業人員資安攻防演練及資安解決方案驗證。

攻防演訓部分，規劃建置模擬系統提供紅隊進行攻擊腳本的發展及模擬，初期先透過模擬系統進行觀察及測試，再導入測試場域，同時可針對電網相關傳輸協定(IEC61850、DNP3、GOOSE、IEC 60870-5-104 等)及特殊專有協定(Emerson、GE、Schneider、三菱等)進行解析及研究。藍隊部分將針對實測場域發生的資安攻擊事件進行事件監控及分析、事件處理、災後復原進行演練。

2. 大學區網中心

提供校園資安教學所需之場域設施，初期優先以已設立資安系所之學校為補助對象，以 TANET 區網中心為實習場域，融入教學實習並進行實作驗證，提供國內大學校院資安實務教學培力場域，規劃如圖 3-5。

圖 3-5：學術場域建置規劃

由學校針對區網中心實體網路環境所面臨之實務資安攻防應用議題，大量部署客制化教學環境，設計資安實務研討課程或專題競賽，快速模擬攻擊與防守角色，鼓勵學生設計並實作可提升區網中心資安防護能量之解決方案，搭配去識別化真實資料，開放場域驗證實驗成果，成果可擇優佈署至現有 13 個區網中心，初期以國立臺灣大學臺北區網中心與國立陽明交通大學桃竹苗區網中心為試辦點，後續視試辦成效評估擴大辦理，如圖 3-6 所示。

圖 3-6：學術場域規劃內容

3. 政府開放場域

主要係以現有 GSN 骨幹網路收容及分析基礎，於資安卓越中心建置合適場域並逐步完備其能量，並協調政府機關開放部份網路或應用系統供資安實習，後續年度視中央及地方政府資安防護需求進行調整，期提供國內學研單位作為資安分析與防護技術之實務研究。

（1）110 年度目標為完備 GSN 骨幹流量收容能力與強化攻擊指標與受害指標行為回溯偵測，關鍵作業項目如下：

A. 完整接收 GSN 骨幹流量達 100Gbps：現有 GSN 骨幹網路已於 108 年中升級內部流量介面至 100Gbps，目前流量介接介面僅能提供 40Gbps 之收容能量，已無法完整收容 GSN 的流量，故有封包丟失的現象產生，有礙於骨幹資安分析與偵防技術之發展，首要解決並完備流量介接之能量。

B. Meta 資料回溯能量達 12 個月：現行 GSN 骨幹網路之資料回溯能量為 3 個月，駭客為躲避資安分析與偵防，APT 攻擊的潛伏期也越來越長，為精進對 APT 攻擊之偵防技術，強化攻擊指標與受害指標行為並拉長回溯偵測，有助於在威脅影響運作前掌握攻擊威脅樣態，降低受害的威脅，具體成果為提升 Meta 資料回溯能量達 12 個月。

C. 完整收容 DNS 與惡意郵件流量之封包層惡意行為偵測/分析資料回溯能量達 12 個月：DNS 資安問題已經隨著

現今各式網路服務應用成長而不斷攀升，以 DNS 基礎的攻擊類型，包括 DNS 服務癱瘓攻擊、反射/放大攻擊、中間人攻擊、偽冒嫁接、惡意程式、殭屍網路、資料外洩通道等，一般 APT 攻擊大部分透過社交工程或電子郵件的方式進行散播、感染最後進行資料竊取。提供 DNS 與惡意郵件流量之封包層惡意行為偵測/分析資料回溯能量達 12 個月，有助於分析各種的 DNS 威脅與偵測電子郵件中的 APT 攻擊。

(2) 111 年度目標為政府開放場域基礎環境暨實驗室建置與政府開放場域營運制度建立，關鍵作業項目如下：

A. 建置政府開放場域主要機房與資安實習實驗室：面對資安事件發生頻率日益升高，不法份子的攻擊手法日新月異，藉由真實的 GSN 骨幹流量資料，學習如何執行樣本分析，增加學習萃取字串與流量特徵經驗，提升機關(構)人員對資安偵防之分析能量，建置政府開放場域主要機房與資安實習實驗室。政府開放場域基礎環境建設，包含機房相關設施建置、資安實習實驗室建置、網路與資安防禦系統軟硬體建置及 OA 設備建置等項目。

B. 政府開放場域營運制度建立：在規劃建置期間和長期營運期間，提供穩定營運管理之規劃和細部規格，滿足服務水準和永續營運發展的需求，訂定營運管理制度包含建立內部資通安全稽核組織及其職掌、建立營運管理組織架構及其職掌及建立各項標準作業程序。

(3) 112 年度目標為完備並開放 3 個月政府場域資料供產學研究，關鍵作業項目如下：

A. 建置威脅情資加值分析/索引系統：達成 Log 收集和分析，透過此平台上即可做到管理與查詢所有設備的日誌，方便人員在查測資安問題與分析資安威脅的時間與執行效率。

B. 建置並開放回溯 Meta 資料能量達 3 個月，供產學研究：藉由收集現行 GSN 骨幹網路連線之 Metadata，以大數據分析之方式，來偵測網路上的惡意程式或非善意的

行為，例如偵測DNS Hijacking，或運用HTTP Return Codes找出惡意網站,初期開放3個月Meta資料能量，供產學研究之用。

C. 建置並開放回溯DNS封包層惡意行為偵測/分析資料能量達6個月，供產學研究：如今DNS造成的資安風險正日漸升高，無論是DNS DDoS，或者透過DNS查詢與C&C主機通訊，甚至是利用DNS洩露資訊，都顯示DNS正成為新的資安威脅工具。提供6個月DNS封包層惡意行為偵測/分析資料，分析並瞭解正常流量的常態，察覺出差異點藉以發掘惡意的連現行為。

(4) 113 年度目標為提供機關人員資安實習環境與擴充政府開放場域環境實驗能量達6個月，關鍵作業項目如下：

A. 建置可模擬機關網路環境與應用系統之實驗場域供資安實習：提升政府機關面對網路攻擊之應處能力，有效掌握資安事件，提升應變速度，降低可能造成之損害，建置可提供機關人員資安實習環境，藉以精進資安威脅分析之能力。

B. 擴增並開放回溯Meta資料能量達6個月：因應資安攻擊的潛伏期越來越長，擴增政府開放場域環境實驗能量達6個月，透過長時間之資料回溯能量，有助於發掘更多的資安威脅事件。

C. 新增並開放回溯惡意郵件封包層惡意行為偵測/分析資料能量達6個月：惡意郵件為APT攻擊的關鍵媒介，藉由封包層之網路底層資料，能更精準的進行惡意行為偵測與分析。

(四)國際合作交流

合作對象以美國、歐洲及澳洲等國家級或以資安著名之研究機構為合作對象，初期不排除以鎖定資安重點學校，後續逐步擴展至國家實驗室或標準制定機構等方式辦理，另參與國際組織進行資安標準制定、辦理大型國際學術會議發表研究成果等亦為國際合作內容；在跨國研究之方式暫以共同對特定主題進行互補性合作研究為主。

(五)技術移轉創新育成

本計畫係針對國家任務導向型研究及關鍵核心研究所自行研發產出具發展潛力及市場價值之成果，透過技術移轉方式，幫助國內業者提升技術能力或成立新創公司，本項標的為資安卓越中心自有技術，非經濟部所執行之全面性產業輔導，所以本計畫強調係協助本中心技術轉移成立之公司，利用經濟部、國發會、國科會等既有新創扶助資源，逐步壯大規模，站穩市場，進軍國際；本項工作係提供資安卓越中心用以行銷推廣、輔導培育、場地設施租賃等相關業務所需。

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

數位發展部組織法已三讀通過，後續配合行政法人國家資通安全研究院設立，將密切與相關部會合作協商以妥善安排後續業務交接與銜接方案。

四、與以前年度差異說明

114 年計畫與前期計畫(112-113 年度)之預期關鍵成果差異分述如下：

年度 差異項目	112-113 年度	114 年度
工控場域建置	● 112 年及 113 年每年皆建置 1 個工控場域，並設置攻防技術檢測實驗室，培訓高階學員 30 人。	● 持續擴大攻防技術研發實驗室及攻防技術檢測實驗室能量，培訓高階學員 15 人。
政府開放場域	● 112 年建置威脅 情資加值 分析/索引系統，開放 3 個月政府骨幹網路 Meta data 資料量，供產學研究 ● 113 年建置可模擬機關網路環境與 應用系統之實驗場域，並擴增 開放政府骨幹網路 Meta data 資料量。	政府開放場域為 110-113 年之工作項目，114 年度無訂定相關績效指標，先前年度之延續性進度說明如下： ● 110 年 ✓ 於 GSN(政府網際服務網)臺北網路中心進行政府骨幹網路流量介接，產製流量中介情資，提供惡意行為回溯能量，現行 DNS 回溯能量由 3 個月提升至 1 年。 ● 111 年 ✓ 完成政府骨幹網路實驗場域相關軟硬體及服務，萃取 3 個月政府骨幹實際流量做為實驗資料，供產學單位進

		行網路流量相關實驗驗測。 ● 112 年 ✓ 完成政府網路威脅分析實驗室建置，提供場域供產學研單位進行相關資安研析與驗證，並針對外部單位申請場域研析之申請資格與目的，彙整評選標準。
國際合作	● 112 年對接國外頂級資安技術或研究機構累積達 3 家，113 年則累積達 4 家。 ● 113 年辦理大型國際資安學術或技術會議，參與人數至少 200 人。	國際合作為 110-113 年之工作項目，114 年度無訂定相關績效指標，先前年度之延續性進度說明如下： ● 110 年與加州大學柏克萊分校長期網路安全研究中心(Center for Long-Term Cybersecurity, CLTC)簽訂合作意向書。 ● 111 年 ✓ 與德國馬克斯普朗克安全及隱私研究所(MPI-SP)簽訂 MoU。 ✓ 與日本情報通信研究機構(NICT)簽訂 MoU(輪簽階段)，並向 NICT 展示以藍軍為主的攻防平台，並邀請日本 NICT 與 SecHack365 校友參與資安防禦競賽。 ✓ 辦理 2022 年第 12 屆量子密碼學國際會議。 ● 112 年 ✓ 完成對接國外頂級資安技術或研究機構共計 5 家，並與其中 3 家簽署合作備忘錄(立陶宛創新局、美加州大學柏克萊分校、德國馬克斯·普朗克安全與隱私研究所)，持續接軌國際資安發展及擴大合作。 ✓ 與日本情報通信研究機構(NICT)、資通安全研究與教學中心、國科會臺灣資安科技研究中心共同辦理「2023 TWN-NICT Cybersecurity Workshop」，並邀請 NICT 與

		SecHack365 校友參與網路威脅防禦競賽。
人才培訓	● 112 年及 113 年分別培訓國內及國際實戰人才至少 125 人。 ● 113 年完成自主頂尖資安實戰課程國際化，並開始對國際招生，至少招收國際學生 20 人。	● 訓國內及國際實戰人才至少 60 人。
技術移轉與創新育成	112 年及 113 年無訂定技術移轉與創新育成績效指標。	● 頂尖研究團隊完成技術轉移達 2 件。 ● 頂尖研究團隊完成專利達 2 件。

五、跨部會署合作說明

本計畫在業務分工部分未有跨部會署合作項目，惟本處負責掌理國家資通安全之政策研議、法案審查、計畫核議、業務推動、督導及管考等業務，本計畫部分內容涉及相關部會，如資安前瞻研究、頂尖實戰人才養成、國際合作交流、技術移轉創新育成、大學區網中心實習場域及工控場域建置等，將委請國科會、教育部及關鍵基礎設施主管部會協助辦理。

六、與本計畫相關之其他預算來源、經費及工作項目

無。

肆、前期重要效益成果說明

一、分年度重要執行成果

110 年度重要執行成果如下：

(一)資安前瞻研究：完成資安威脅情資報告 12 篇、期刊論文 9 篇、研討會論文 4 篇、技術論文(尚未發表)7 篇、產業研究政策報告 5 篇、4 套後量子密碼自動化驗證工具、6 個同態加密技術、1 個社群網路資料平台及提供威脅情資平台服務。

(二)頂尖實戰人才養成：建立 1 套共 36 門資安培訓模組化課程(含 7 門管制課程)，並辦理資安菁英班與網路威脅防禦競賽，共培訓 55 名學員，51 名通過評測，並建置以藍軍為主的紅藍攻防平台供競賽及訓練使用。

(三)實習場域建置：以中油大林煉油廠之煉油訓練實習場域做為 OT 場域，搭配技服中心自建 IT 虛擬場域，將 OT 場域與 IT 場域整合，模擬能源領域之真實環境，並以此虛擬場域培訓 21 名學員；另為提供校園資安教學所需之場域設施，以已設立之區網中心為實習場域融入教學實習並進行實作驗證，於臺北區網中心規劃建置區網封包蒐集系統，桃竹苗區網中心開設 EC-Council Certified Ethical Hacker (CEH)駭客技術專家認證課程，共有 32 名學員完成培訓；為以政府骨幹網路為基礎，發展網路流量與威脅分析技術，以供學員實務分析與學習使用，將政府骨幹網路基礎頻寬架構提升至 100G，擴充介接能量至 100G 流量。

(四)國際合作：與加州大學柏克萊分校長期網路安全研究中心(Center for Long-Term Cybersecurity, CLTC)簽訂合作意向書。

(五)技術移轉與創新育成：完成技術移轉與創新育成評估報告 2 篇，並舉辦產業座談會。

111 年度重要執行成果如下：

(一) 資安前瞻研究：完成威脅情資報告 28 篇、國家任務導向型報告 5 篇、研討會論文 4 篇、技術論文(尚未發表)16 篇、CVE 漏洞挖掘揭露報告 12 篇、惡意程式分析平台、更新「社群網路資料平台」為「網路社群分析平台」、異常資訊分析平台、深度偽造影音分析平台、網路大數據資料庫、維運威脅情資平台。

(二) 頂尖實戰人才養成：

1. 完成紅藍攻防平台腳本3套、完成資安課程擴充13類主題，共64門課程。
2. 完成高階實戰人才培訓通過84人、國家級資安戰隊成員已培訓55人。
3. 完成高階學員工控資安實戰課程培訓，本課程受訓對象涵蓋產、政、軍及學等領域，共計30人。
4. 辦理國際資安講座，參與人數18人。

(三) 實習場域建置：

1. 完成台水公司新營員工訓練園區水資源工控模擬場域建置，參考台水公司現有網路架構環境，整合 IT 場域與 OT 場域，並透過演練平台即時呈現演練過程。
2. 完成政府開放場域機房與資安實習實驗室建置，提供場域供產學研單位進行相關資安研析與驗證。
3. 於臺大、陽明交大之區網中心各建置1個資安教學實習場域，於臺大完成區網封包蒐集與鑑識系統及資安大數據分析平臺建置，並開辦30小時資安大數據分析課程；於陽明交大開設40小時 EC-Council Certified Ethical Hacker (CEH)駭客技術專家認證課程，共20名通過證照考試。

(四) 國際合作：

1. 與德國馬克斯普朗克安全及隱私研究所(MPI-SP)簽訂 MoU。
2. 與日本情報通信研究機構(NICT)簽訂 MoU(輪簽階段)，並向 NICT 展示以藍軍為主的攻防平台，此外邀請日本 NICT 與 SecHack365 校友參與資安防禦競賽。
3. 辦理2022年第12屆量子密碼學國際會議。

(五) 技術移轉與創新育成：完成產業評估報告 3 篇，並舉辦 2 場產業座談會及 3 場產業交流會。

112 年度重要執行成果如下：

(一) 資安前瞻研究：完成期刊論文 1 篇(已投稿)、研討會論文 5 篇和技術論文 3 篇，共 9 篇論文報告。

(二) 頂尖實戰人才養成：

1. 開放工控資安之實戰課程訓練教材1套，內含 ICS 資安威脅趨勢與威脅、滲透測試實作、DMZ 攻防演練、內網滲透攻防演練、ICS

基礎與 PLC 程式設計、HMI 基礎程式實作、內網橫向擴散攻防演練、ICS 攻防演練等8門課程，以符合資安實務培訓所需。

2. 辦理資安菁英人才培訓課程，培訓具國際競爭力之資安實戰菁英人才，以政府單位資安技術人員、企業資安技術人員、資安公司研發人員為主，開設3期實務課程，計164人取得證書。
3. 組成國家資安聯隊 TWN48，參加2023世界駭客大賽(DEF CON)搶旗攻防賽(CTF)獲得全球第三名。

(三)實習場域建置：

1. 臺北醫學大學偕同附屬醫院完成醫療場域建置，提供國內資安防護解決方案之實證場域，並支援教育訓練及攻防演練使用。同時舉辦工控資安實戰課程，受訓對象涵蓋產、政、軍及學等領域，計39位學員取得證書。
2. 完成政府骨幹網路實驗場域相關軟硬體及服務，萃取3個月政府骨幹實際流量做為實驗資料，供產學單位進行網路流量相關實驗驗測。

(四)國際合作：

1. 完成對接國外頂級資安技術或研究機構共計5家，並與其中3家簽署合作備忘錄(立陶宛創新局、美加州大學柏克萊分校、德國馬克斯·普朗克安全與隱私研究所)，持續接軌國際資安發展及擴大合作。
2. 與日本情報通信研究機構(NICT)、資通安全研究與教學中心、國科會臺灣資安科技研究中心共同辦理「2023 TWN-NICT Cybersecurity Workshop」，並邀請 NICT 與 SecHack365校友參與網路威脅防禦競賽。

(五)技術移轉與創新育成：完成創新技術 2 項，並已被相關單位採用，已著手與有意願之單位簽署 MOU 並辦理後續技術移轉事宜。

二、里程碑達成情形

110-112 年度各項里程碑均如期如質完成，113 年度計畫刻正執行中，各項指標完成情形如下表：

(一)工作指標

項次	指標項目	單位	【計畫全期】總目標值	【累計至112年】	
				目標值	實際值
1	建置工控場域	個	4	3	3
2	接收 GSN 骨幹網路流量	G	100	100	100
3	現行 DNS 回溯能量	年	1	1	1
4	辦理1場大型國際資安學術或技術會議之參與人數	人	200	200	1,137
5	區網中心建置為資安高階教學實習場域	個	2	2	2
6	模組化資安課程	套	1	1	1
7	與國際知名的資安研究中心或國際組織簽訂合作意向書以上之協議	家	4	3	3

(二)效益指標

項次	指標項目	單位	【計畫全期】總目標值	【累計至112年】	
				目標值	實際值
1	研究報告、期刊論文、研討會論文或威脅情資報告	篇	36	9	111
2	高階實戰人才培育	人	410	125	264
3	工控場域實戰人才培育	人	125	20	90
4	技術轉移	件	2	0	0
5	研究完成專利	件	2	0	0

三、可量化經濟效益

本計畫先期於 110 年 9 月起招募研究人員與行政人員 23 名，自國家資通安全研究院 112 年成立並整併前技術服務中心與資安卓越中心業務以來，現 113 年研究人員人數已達 200 人，增加 177 人之就業機會。

四、不可量化經濟效益

(一)研發資安尖端技術

藉由推動資安前瞻研究，於國際研討會或國際期刊發表，提升國際知名度和影響力，吸引全球專業人才加入，使研究團隊多元化，進而提升研究質量與創新性，並研發資安尖端技術，鞏固我國在全球資訊安全領域的地位，活絡本國資安產業。

(二)培養潛在資安從業人員

結合資安新興威脅及趨勢發展開設資安實作攻防課程與實戰演練，提升學員實戰經驗，培育國內所需資安高階人才，活絡本國資安產業。

(三)降低資安風險

1. 透過實驗場域所得之政府骨幹實際流量做為實驗資料，有助於改善以機器學習、大數據分析等方法之效能表現，以提升產學單位相關偵測系統之有效性。
2. 藉由資安實作攻防課程與實戰演練經驗，提升產官學研各界資安防護能量，降低資安風險及可能造成的經濟損失。

伍、預期效益及效益評估方式規劃

成立資安卓越中心之目的在解決國內高階資安人才不足的問題，長期目標係成為亞太高階資安人才及技術創新基地，其功能包括資安前瞻研究、頂尖實戰人才養成、實習場域建置、國際合作交流、技術移轉創新育成等5項主要功能，預期效益重點說明如下：

1. 擇優挑選產學政軍之人才進行培訓，透過「以戰代訓」之理念，定期密集針對不同模擬場域進行實戰演練，提升學員實戰經驗，完訓獲得較優渥之就業機會，並做為國家緊急需調用人力之後盾，長期招收對象將擴及亞太地區。
2. 因應資安新興威脅及趨勢發展，由資安卓越中心延聘國際優秀人才，負責政府機關短中期所需之應用技術研究，以及國家長期關鍵核心之基礎研究，以培育並厚植我國資安前瞻研究自主能量；同時參與國際資安標準規範制定，確保開發技術與國際接軌，除可透過技轉方式，幫助國內業者提升技術能力或成立新創公司，亦可藉由資安前瞻研究成果進行國際合作，提升台灣國際能見度。
3. 於資安卓越中心建置國家型工控場域，提供國內關鍵基礎設施領域所需資安防護解決方案之實證場域，並支援教育訓練及大型攻防演練，另透過補助大學區網中心提供校園資安教學所需之場域設施，以及協調政府機關開放部份網路或應用系統供資安實習，拓展資安教學實習場域，完善資安教學設備環境。

本計畫效益評估方式採「過程型」之工作指標與「成果型」之效益指標，工作指標依每年度預期關鍵成果之里程碑檢視是否達成當年度目標；效益指標則以本計畫所完成之資安前瞻研究成果(含論文及報告數量、技術轉移及專利申請件數等)及高階資安人才培育人數進行評估，如下表：

(一)114年工作指標

項次	指標項目	單位	114年目標值
1	高階實戰人才培育	人	15
2	工控場域實戰人才培育	人	60
3	技術轉移	件	2
4	研究完成專利	件	2

(二)計畫全程效益指標

項次	指標項目	單位	114年目標值	【計畫全期】總目標值
1	研究報告、期刊論文、研討會論文或威脅情資報告	篇	-	36
2	高階實戰人才培育	人	15	410
3	工控場域實戰人才培育	人	60	125
4	技術轉移	件	2	2
5	研究完成專利	件	2	2

陸、自我挑戰目標

年度	目標	原訂目標值	挑戰目標	達成情形
114 年	O1KR1	原訂為「工控場域培訓高階學員達 15 人」，挑戰目標增加為培訓學員達 20 人。	增加為培訓學員達 20 人	-
	O3KR2	原訂為「邀請國外資安學界、業界和社群知名人士結合工控場域培訓國內實戰人才至少 60 人」，挑戰目標增加為培訓學員達 75 人。	增加為培訓學員達 75	-
113 年	O3KR2	原訂為「邀請國外資安學界、業界和社群知名人士結合工控場域培訓國內及國際實戰人才至少 125 人」，挑戰目標增加為培訓學員達 150 人。	增加為培訓學員達 150 人	計畫刻正執行中。
112 年	O1KR1	原訂為「持續建置工控場域累積達 3 個，並設置攻防技術研發實驗室，培訓高階學員達 30 人」，挑戰目標增加為培訓學員達 40 人。	增加為培訓學員達 40 人	工控資安實戰課程共計培訓 42 位學員，其中 39 位學員取得證書。
	O3KR2	原訂為「邀請國外資安學界、業界和社群知名人士結合工控場域培訓國內實戰人才至少 125 人」，挑戰目標增加為培訓學員達 150 人。	增加為培訓學員達 150 人	資安菁英人才培訓 3 期課程辦，計 480 位報名，經錄取培訓國內資安實戰人才 180 人，164 人取得證書。扣除政府單位，共培育產業資安及資安產業 129 人。

柒、經費需求/經費分攤/槓桿外部資源

經費需求表(B005)

單位：千元

細部計畫名稱	計畫屬性	114 年度(8 月)		
		小計	經常支出	資本支出
臺灣資安卓越深耕-資安卓越中心計畫	C.人才培育	158,000	126,400	31,600

A. 組織維運/類業務：常態性支持與維運法人組織運作，或為支持科研發展衍生之常規性業務或研究等計畫。

B. 資通訊建設：以資通訊設備建置為計畫核心，目的在於推動資訊化社會之建設，建構完善基礎環境，規劃資訊通信關鍵應用，以帶動資訊國力提升。

C. 人才培育：計畫主軸係以人才培育為核心策略，以人力資本的投入帶動基礎研究、產業發展或轉型及公共民生之發展。

D. 基礎研究：非以專門或特定應用/使用為目的，成果不特別強調與產業的連結性；或為目前已知或未來預期面臨之問題，但尚缺乏廣泛知識基礎而進行之研究。本屬性涵蓋基礎研究核心設施。

E. 產業技術研發：進行與產業連結性高之相關技術研究與開發。

F. 產業服務與應用：將科技研究與技術應用於產業，進而推動產業發展，包括技術及產品應用或產業輔導等。

G. 環境永續與社會發展：具永續性或有助於民生及公共福祉之公共資源、公共服務、科技政策等，於短、中、長期可促進各類人民福祉之提升、環境之保全與安全之促進。

114 年度經費需求表

經費需求說明

本計畫以「成為亞太高階資安人才及技術創新基地」為目標，設立資安卓越中心，從資安前瞻研究、頂尖實戰人才養成、實習場域建置、國際合作及技術移轉創新育成等5個面向著手，挹注充足教學及研究資源，以厚植我國頂尖實戰人才培訓及資安前瞻研究能量，114年經費需求1.58億元。

114 年度經費需求表

單位：千元

計畫名稱	細部計畫重點描述	預期關鍵成果	114 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
臺灣資安卓越深耕-資安卓越中心計畫	1. 持續擴大工控場域攻防技術能量 2. 推動本國資安高等研究成果落地 3. 持續擴大國內頂尖實戰資安人才培訓能量	1. 持續擴大攻防技術研發實驗室及攻防技術檢測實驗室能量，並用於國內高階實戰人才培育 2. 工控場域培訓高階學員達 15 人	158,000	0	0	126,400	0	0	31,600

		3. 頂尖研究團隊完成技術轉移達 2 件 4. 頂尖研究團隊完成專利達 2 件 5. 邀請國外資安學界、業界和社群知名人士結合工控場域培訓國內及國際實戰人才至少 60 人							

經費分攤表(B008)

無經費分攤。

捌、儀器設備需求

無儀器設備需求。

玖、就涉及公共政策事項，是否適時納入民眾參與機制之說明

無涉及公共政策事項。

拾、附錄

一、政府科技發展計畫自評結果(A007)

(一)計畫名稱：臺灣資安卓越深耕-資安卓越中心計畫
審議編號：114-5010-09-20-01
計畫類別：前瞻基礎建設計畫

(二)自評委員：李榮三、羅金賢、馬正維

日期：113 年 5 月 24 日

(三)審查意見及回復：

序號	審查意見	回復說明
1	資安前瞻之關鍵核心研究包含網路威脅防禦、網路數據分析及先進密碼研究，除了發掘潛在網路威脅，打造安全網路空間，更預先佈防安全密碼系統以因應量子運算所帶來之挑戰。	感謝委員支持。
2	前期計畫成果皆有超出預期目標，本期延續之年度工作目標明確，包含持續擴大工控場域攻防技術能量、推動資安高等研究成果落地以及持續擴大國內頂尖實戰資安人才培訓能量。尤其，部分成果目標亦已適時向上調整，在年度挑戰目標的部分，培訓高階學員人員數由 15 人提升至 20 人，培訓國內實戰人才數量由 60 人增加至 75 人。	感謝委員支持。
3	對於頂尖人才及前瞻研究人才培育，建議納入高教資安相關師資之養成，並挹注充足教學及研究資源。資安教師數量增加應能強化國人資安素養並提	謝謝委員建議，本計畫目標在培育頂尖資安實戰人才，經查高教資安相關師資之養成係由教育部主政，本署主提另一支跨部會科技計畫

	升大專院校中資安璞玉發掘之可能。	「資安跨域整合聯防計畫」中，細部計畫教育部已在辦理大專校院資安實務種子教師研習營，分享資安實務示範課程教案設計與教學經驗，培育跨領域資安種子師資，並優化大專校院資安實務課程教學設計與應用，擴散資安實務課程教學能量。 114 年教育部更預計擴大既有資安實務示範課程使用以及跨領域資安種子師資培訓，將學校資安實務教學能量推廣至全國大專校院，並參考 ACM 之資安人才培育課程建議，提出適合臺灣之資安課程，完善相關課程模組教學資源。 本署 114 年之科技計畫已分配經費支持教育部持續推動資安師資培育及充實教學資源，以厚植我國頂尖實戰人才培訓能量。
4	可行性評估：114 年計畫之目標，係持續擴大工控場域攻防技術能量，推動本國資安高等研究成果落地，並持續擴大國內頂尖實戰資安人才培訓能量，符合長期資安人才培育之目標與策略，且前期計畫已有具體成果，顯示其延續性及實施之可能性。	感謝委員支持。
5	預期效益:本計畫預計將解決國內高階資安人才不足的問題，並成為亞太地區的資安人才及技術創新基地，對國家的數位安全及產業發展具長遠的正面影響。並透過國際合作及技術移轉，使計畫有助於提升台灣在全球資安領域的能見度及競爭力。	感謝委員支持。

6	創新價值:本計畫亦提出多面向的執行策略,包括前瞻研究、實戰人才培訓及國際合作等,此為資安領域內創新發展的關鍵要素。尤其技術移轉及創新育成,將有助於促進新創公司的成立及技術創新,對推動國家整體科技創新生態系具正面的影響。	感謝委員支持。
7	1-1 頁:計畫目標及預期關鍵成果之「目標 2:推動本國資安高等研究成果落地關鍵成果 1:頂尖研究團隊完成技術轉移累積 2 件 關鍵成果 2:頂尖研究團隊完成專利累積 2 件」,因僅屬 114 年度之目標值,建議修正為至少 2 件或達 2 件。其他 1-4 頁、3-16 頁及 5-2 頁之(一)114 年工作指標之累計,宜一併修正之。	謝謝委員建議,已調修相關文字。
8	5-2 頁:(二)計畫全程效益指標,僅呈現【計畫全期】總目標值,建議增加一欄位為 114 年目標值,以呈現 114 年各指標項目之量化值。	感謝委員建議,114 年目標值已補充於 5-2 頁(上傳版本為 44 頁)。
9	實習場域建置包括「工控場域」、「大學區網中心」及「政府開放場域」,除以人數作為人才培育之目標值外,建議評估各場域使用率作為工作指標之可行性。	謝謝委員建議,「政府開放場域」於 113 年開放營運,預訂開放場域申請對象為與資安相關之產學單位,114 年計畫執行目標並無「政府開放場域」工作項目,惟後續可評估將場域申請使用情形(如場域申請之研究團隊數)納入計畫執行目標之可行性,並於績效報告中說明。 另有關「工控場域」及「大學區網中心」,其場域建置完成後續會移交予所屬單位,由該單位自行規劃運用,辦理符合該領域所需之資安

		人才培訓或攻防演練，執行情形分述如下： 1. 大學區網中心係 110-111 年委請教育部辦理，於臺大、陽明交大之區網中心各建置 1 個資安教學實習場域，現區網中心已移交由學校後續進行資安人才培訓，114 計畫已無大學區網中心工作項目。 2. 本計畫 110-113 年每年建置 1 座工控實習場域，同時利用該場域辦理攻防演練及工控資安實戰課程。後續規劃將實習場域移交給該關鍵基礎設施提供者，善用既有工控模擬環境辦理資安演練、訓練符合該領域所需資安實戰人才，作為該領域資安實務人才生態之實訓場域。
10	本(114)年度計畫為全程計畫期程之最後一年，全程計畫推動項目包含資安前瞻研究、頂尖實戰人才養成、實習場域建置等，建議可將全程計畫之具體推動成效，納入本年度期末報告中，並進行相關研析及檢討。	謝謝委員建議，本計畫全程目標包含資安前瞻研究、頂尖實戰人才養成、工控場域建置、跨國合作等作為，將於 114 年之績效報告中呈現並說明計畫全程各項作為之具體推動成果，並進行相關研析及檢討。
11	p3-16 本年度計畫中對於「政府開放場域」及「國際合作」未有說明，建議可將先前年度之延續性進度，納入此部分中說明。	謝謝委員建議，3-16 頁原係呈現計畫前期(112-113 年)及 114 年預期關鍵成果之差異說明，其中計畫全程目標規劃「政府開放場域」及「國際合作」為 110-113 年之重點工作，114 年為本計畫最後一年，關鍵成果著重於持續培訓頂尖實戰資安人才，並推動具發展潛力、產業價值之高等研究成果落地。惟為呈現先前年度之延續性進度，已依委員建議將執行成果補充於 3-16 頁(上傳版本為 35-37 頁)。

12	本計畫各項推動成果誠屬不易，後續建議建立相關成果之追蹤機制，對各項成果之後續發展及進程進行追蹤分析，如人才培訓學員之就業、就職情形，工控場域之使用及擴充狀況，簽署之合作備忘錄進一步之合作成果等，應可更彰顯本計畫之價值。	謝謝委員建議，本計畫推動相關作為之同時，亦有考量後續發展之實質成效，以彰顯各項成果之價值。目前相關成果後續發展分述如下： 1. 人才培訓學員追蹤：113 年預計針對前一年度培訓之學員進行流向調查，以評估課程實訓對於學員職業發展的影響，以及對資安業界或關鍵基礎設施資安社群之技術及人才貢獻度，據以進一步精進和完善課程設計。 2. 工控場域使用：本計畫評估各關鍵基礎設施人才需求之迫切性、需求性等，每年建置一座工控場域，並辦理資安實戰培訓課程，未來主要作為教育訓練及攻防演練所需。此外，111 年建置水資源工控場域作為 112 年跨國攻防演練(CODE 2023)場域，112 年建置醫療工控場域將規劃作為 114 年跨國網路攻防演練(CODE 2025)場域。後續會將場域移交給所屬關鍵基礎設施提供者，期善用善用既有工控模擬環境辦理該領域所需之資安相關演練。 3. 國際合作：積極與已簽屬 MOU 之產學界研究機構緊密交流洽談實質合作，包含： ● 110 年與加州大學柏克萊分校長期網路安全研究中心(CLTC)簽訂 MOU，111 年推動「2030 網路安全展望」台灣站以及台灣學者短期移地研究等項目，112 年推動「資安人才培育及資安意

		識推廣經驗、教材及工具」與「AI 安全政策及國際 AI 相關法規」等項目，與 CLTC 建立長期合作架構，進行資訊交流分享及相關研究合作。 ● 111 年與日本情報通信研究機構(NICT)開啟雙邊合作，連續 2 年邀請 NICT SecHack365 校友隊參與網路威脅防禦競賽，112 年共同辦理「TWN-NICT Cybersecurity Workshop」，資安技術及相關應用研發進行交流與合作討論，擴增我國資安人培之國際視野。 ● 111 年與德國馬克斯普朗克安全及隱私研究所(MPI-SP)簽訂 MOU，建立長期合作架構，可共同開發技術，瞭解他國資安領域發展。112 年本計畫開發後量子加密驗證工具 CryptoLine，已被 MPI-SP 資助之 Formosa Crypto 計畫決議採用，並邀請我方研究人員分別於參與會議共同討論工具整合。

第五點附表一--中長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10點)	V		✓		
	(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		✓		
	(3)是否本於提高自償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		✓	
2、民間參與可行性評估	(1)是否評估民間參與之可行性，並撰擬評估說明(編審要點第4點)		V		✓	
	(2)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		✓	
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		✓	
	(2)是否研提完整財務計畫		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		✓		
	(2)資金籌措：本於提高自償之精神，將影響區域進行整合規劃，並將外部效益內部化		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、本於提高自償之精神所擬訂各類審查及補助規定	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		✓		
	(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		✓	
	(6)屬具自償性者，是否透過基金協助資金調度		V		✓	
5、人力運用	(1)能否運用現有人力辦理	V		✓		
	(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		✓	
6、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		✓	
	(2)是否檢附相關協商文書資料		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	
7、土地取得	(1)能否優先使用公有閒置土地房舍		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		✓	
	(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		✓	
	(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		✓	
	(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			
8、風險管理	是否對計畫內容進行風險管理	V		✓		
9、性別影響評估	是否填具性別影響評估檢視表	V		✓		
10、環境影響分析(環境政策評估)	是否須辦理環境影響評估		V		✓	
11、淨零轉型通案評估	(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		✓	
	(2)是否規劃採用綠建築或其他節能減碳措施		V		✓	
	(3)是否強化因應氣候變遷之調適能力，並納入淨零排放及永續發展概念，優先選列臺灣2050淨零排放路徑、淨零科技方案及淨零轉型十二項關鍵戰略、臺灣永續發展目標及節能相關指標		V		✓	
	(4)是否屬臺灣2050淨零排放路徑、淨零科技方案及淨零轉型十二項關鍵戰略相關子計畫		V		✓	
	(5)屬臺灣2050淨零排放路徑、淨零科技方案及淨零轉型十二項關鍵戰略之相關子計畫者，是否覈實填報附表三、中長程個案計畫淨零轉型通案自評檢核表，並檢附相關說明文件		V		✓	
12、涉及空間規劃者	是否檢附計畫範圍具座標之向量圖檔		V		✓	
13、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		✓	
14、落實公共工程或房屋建築全生命週期各階段建造標準	是否瞭解計畫目標，審酌其工程定位及功能，對應提出妥適之建造標準，並於公共工程或房屋建築全生命週期各階段，均依所設定之建造標準落實執行		V		✓	
15、公共工程節能減碳及生態檢核	(1)是否依行政院公共工程委員會(下稱工程會)函頒之「公共工程節能減碳檢核注意事項」辦理		V		✓	
	(2)是否依工程會函頒之「公共工程生態檢核注意事項」辦理		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	
16、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		✓	
17、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		✓	
18、營(維)運管理計畫	是否具務實及合理性(或能否落實營運或維運)	V		✓		
19、房屋建築朝近零碳建築方向規劃	是否已依工程會「公共工程節能減碳檢核注意事項」及內政部建築研究所「綠建築評估手冊」之綠建築標章及建築能效等級辦理		V		✓	
20、地層下陷影響評估	屬重大開發建設計畫者，是否依「機關重大開發建設計畫提報經濟部地層下陷防治推動委員會作業須知」辦理		V		✓	
21、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		✓		

主辦機關核章：承辦人 潘偉庭 8806　單位主管 林郁傑　首長 數位發展部資通安全署署長 謝翠娟(甲)

主管部會核章：研考主管 數位策略司司長 蔡壽注　會計主管 主計處處長 李錫東　首長 數位發展部部長 黃彥男(丙)

三、性別影響評估檢視表

本計畫屬已核定之中長程個案計畫，修正或補充內容僅限於調整計畫執行之細節性或技術性事項，爰依「行政院所屬各機關中長程個案計畫編審要點附表 2：中長程個案計畫性別影響評估作業說明」第 3 點規定，免重辦性別影響評估，並檢附前次辦理之性別影響評估檢視表如下：

中長程個案計畫性別影響評估檢視表【一般表】

【第一部分】：本部分由機關人員填寫

【填表說明】各機關使用本表之方法與時機如下：

一、計畫研擬階段

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

（二）請運用本表所列之評估項目，將性別觀點融入計畫書草案：

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

二、計畫研擬完成

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

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

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

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

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

計畫名稱：臺灣資安卓越深耕			
主管機關 （請填列中央二級主管機關）	數位發展部	**主辦機關（單位）** （請填列擬案機關／單位）	數位發展部資通安全署

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）。	因應國際性別主流化潮流，推動性別平等政策綱領，建構性別友善職場環境，鼓勵女性參與決策，於各層級合議式決策機制(委員會)內，應不低於 1/3 比例，以追求平等參與、破除性別隔離，讓男女能平等參與決策，減少因性別而帶來的知識與技術落差，並鼓勵女性成為意見領袖，重視女性與弱勢者的經驗、知識和價值。

評估項目	評估結果
1-2【請蒐集與本計畫相關之性別統計及性別分析（含前期或相關計畫之執行結果），並分析性別落差情形及原因】 請依下列說明填寫評估結果： a.歡迎查閱行政院性別平等處建置之「性別平等研究文獻資源網」 (https://www.gender.ey.gov.tw/research/)、「重要性別統計資料庫」(https://www.gender.ey.gov.tw/gecdb/)（含性別分析專區）、各部會性別統計專區、我國婦女人權指標及「行政院性別平等會─性別分析」(https://gec.ey.gov.tw)。 b.性別統計及性別分析資料蒐集範圍應包含下列 3 類群體： ①**政策規劃者**（例如:機關研擬與決策人員；外部諮詢人員）。 ②**服務提供者**（例如:機關執行人員、委外廠商人力）。 ③**受益者**（或使用者）。 c.前項之性別統計與性別分析應盡量顧及不同性別、性傾向、性別特質及性別認同者，探究其處境或需求是否存在差異，及造成差異之原因；並宜與年齡、族群、地區、障礙情形等面向進行交叉分析（例如：高齡身障女性、偏遠地區新住民女性），探究在各因素交織影響下，是否加劇其處境之不利，並分析處境不利群體之需求。前述經分析所發現之處境不利群體及其需求與原因，應於後續【1-3 找出本計畫之性別議題】，及【貳、回應性別落差與需求】等項目進行評估說明。	1. 本計畫政策規劃者共 4 人，女性有 2 人占比 50%，已超過 1/3。 2. 本計畫未來機關執行人員將鼓勵女性參與，且參與率應不低於 30%。 3. 本計畫完成後，不以特定性別、性傾向或性別認同者為受益對象。 4. 過去五年(103 年至 107 年)資訊通訊科技領域之畢業生男女性別比率約為 7 比 3。本計畫辦理時，將鼓勵女性參與，且參與率應不低於 30%。

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）。	

評估項目	評估結果
1-3【請根據 1-1 及 1-2 的評估結果，找出本計畫之性別議題】 性別議題舉例如次： **a.參與人員** 政策規劃者或服務提供者之性別比例差距過大時，宜關注職場性別隔離（例如：某些職業的從業人員以特定性別為大宗、高階職位多由單一性別擔任）、職場性別友善性不足（例如：缺乏防治性騷擾措施；未設置哺集乳室；未顧及員工對於家庭照顧之需求，提供彈性工作安排等措施），及性別參與不足等問題。 **b.受益情形** ①受益者人數之性別比例差距過大，或偏離母體之性別比例，宜關注不同性別可能未有平等取得社會資源之機會（例如:獲得政府補助；參加人才培訓活動），或平等參與社會及公共事務之機會（例如:參加公聽會/說明會）。 ②受益者受益程度之性別差距過大時（例如:滿意度、社會保險給付金額），宜關注弱勢性別之需求與處境（例如:家庭照顧責任使女性未能連續就業，影響年金領取額度）。 **c.公共空間** 公共空間之規劃與設計，宜關注不同性別、性傾向、性別特質及性別認同者之空間使用性、安全性及友善性。 ①使用性：兼顧不同生理差異所產生的不同需求。 ②安全性：消除空間死角、相關安全設施。 ③友善性：兼顧性別、性傾向或性別認同者之特殊使用需求。 **d.展覽、演出或傳播內容** 藝術展覽或演出作品、文化禮俗儀典與觀念、文物史料、訓練教材、政令/活動宣導等內容，宜注意是否避免複製性別刻板印象、有助建立弱勢性別在公共領域之可見性與主體性。 **e.研究類計畫** 研究類計畫之參與者（例如:研究團隊）性別落差過大時，宜關注不同性別參與機會、職場性別友善性不足等問題；若以「人」為研究對象，宜注意研究過程及結論與建議是否納入性別觀點。	1. 本計畫決策人員女性比例超過 1/3，機關執行人員將鼓勵女性參與，且參與率應不低於 30%，無性別參與不足等問題。 2. 本計畫完成後，不以特定性別、性傾向或性別認同者為受益對象。 3. 本計畫辦理時，將建議執行機關於公共空間營造性別友善環境，並鼓勵弱勢性別族群參與。

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

評估項目	評估結果
2-1【請訂定本計畫之性別目標、績效指標、衡量標準及目標值】 請針對 1-3 的評估結果，擬訂本計畫之性別目標，並為衡量性別目標達成情形，請訂定相應之績效指標、衡量標準及目標值，並納入計畫書草案之計畫目標章節。性別目標宜具有下列效益： **a.參與人員** ①促進弱勢性別參與本計畫規劃、決策及執行，納入不同性別經驗與意見。 ②加強培育弱勢性別人才，強化其領導與管理知能，以利進入決策階層。 ③營造性別友善職場，縮小職場性別隔離。 **b.受益情形** ① 回應不同性別需求，縮小不同性別滿意度落差。 ② 增進弱勢性別獲得社會資源之機會（例如:獲得政府補助；參加人才培訓活動）。 ③ 增進弱勢性別參與社會及公共事務之機會（例如:參加公聽會/說明會，表達意見與需求）。 **c.公共空間** 回應不同性別對公共空間使用性、安全性及友善性之意見與需求，打造性別友善之公共空間。 **d.展覽、演出或傳播內容** ① 消除傳統文化對不同性別之限制或僵化期待，形塑或推展性別平等觀念或文化。 ② 提升弱勢性別在公共領域之可見性與主體性（如作品展出或演出；參加運動競賽）。 **e.研究類計畫** ① 產出具性別觀點之研究報告。 ② 加強培育及延攬環境、能源及科技領域之女性研究人才，提升女性專業技術研發能力。 **f.**強化與本計畫相關的性別統計與性別分析。 **g.**其他有助促進性別平等之效益。	1. 本計畫係成立資安卓越中心，主要辦理資安前瞻研究、頂尖實戰人才養成、實習場域建置、國際合作及技術移轉創新育成。計畫規劃階段決策人員女性占比已達 50%，未來機關執行人員將鼓勵女性參與，且參與率應不低於 30%，且計畫完成後，不以特定性別、性傾向或性別認同者為受益對象，故本次不另外訂定性別目標。 2. 本計畫辦理時，將建議執行機關了解弱勢性別族群之需求，營造性別友善環境，鼓勵弱勢性別族群參與。
評估項目	**評估結果**
2-2【請根據 2-1 本計畫所訂定之性別目標，訂定執行策略】 請參考下列原則，設計有效的執行策略及其配套措施：	1. 本計畫係成立資安卓越中心，主要辦理資安前瞻研究、頂尖

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。	實戰人才養成、實習場域建置、國際合作及技術移轉創新育成。計畫規劃階段決策人員女性占比已達 50%，未來機關執行人員將鼓勵女性參與，且參與率應不低於 30%，且計畫完成後，不以特定性別、性傾向或性別認同者為受益對象，故本次不另外訂定性別目標及相關策略。 2. 本計畫辦理時，將建議執行機關了解弱勢性別族群之需求，營造性別友善環境，鼓勵弱勢性別族群參與。

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。	本計畫係成立資安卓越中心，主要辦理資安前瞻研究、頂尖實戰人才養成、實習場域建置、國際合作及技術移轉創新育成，且計畫完成後，不以特定性別、性傾向或性別認同者為受益對象，故未編列性別相 關事項經費。

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

參、評估結果

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

<table>
<tr><td>3-1 綜合說明</td><td colspan="2">本計畫係設立資安卓越中心，從資安前瞻研究、頂尖實戰人才養成、實習場域建置、國際合作及技術移轉創新育成等 5 個面向著手，挹注充足教學及研究資源，以厚植我國頂尖實戰人才培訓及資安前瞻研究能量。委員期待以過去三年相關機關推動辦理資安人才培育成果補充說明性別統計及性別分析。</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>無</td></tr>
<tr><td>3-2-2 說明未參採之理由或替代規劃</td><td>過去三年相關機關推動資安人才培育之學員來源，主要來自資通訊科技領域，參考過去五年(103 年至 107 年)資訊通訊科技領域之畢業生男女性別比率約為 7 比 3。本計畫未來成立資安卓越中心之性別平等推動規劃之如下：
(1) 徵求資安前瞻研究人員、實戰型頂尖人才研訓師資及維運資安卓越中心行政所需人力等，應符合資訊領域目前師生之性別比例，並營造性別友善環境，鼓勵弱勢性別族群參與。
(2) 將於未來資安卓越中心全球資訊網，建置性別統計專區或性別主流化專區，積極推動性別主流化。</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：江樫皇 職稱：分析師 電話：02-33568172 填表日期：109 年 7 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：吳嘉麗 服務單位及職稱：淡江大學化學系榮譽教授 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 7 月 28 日 至 109 年 8 月 2 日
2.參與者姓名、職稱、服務單位及其專長領域	吳嘉麗　淡江大學化學系榮譽教授/ 台灣女科技人學會 創會理事長 性別與科技
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	不足，可以再完整
6.本計畫性別議題之合宜性	請見綜合意見
7.性別目標之合宜性	請見綜合意見
8.執行策略之合宜性	請見綜合意見
9.經費編列或配置之合宜性	沒有意見
10.綜合性檢視意見	本計畫之性別統計尚可包含如 P23 及 P24 均提及之下列學員性別統計以及 P25 所提之資安職能證書千餘人之性別統計。 P23 及 P24 …新型態資安暑期課程，每年均有近 500 名大專 校院及高中職學生報名，經過資安實務測驗後， 錄取約 180 名學員參與 AIS3 課程。…..。 3. 高階資安：資安實務導師培訓(臺灣好厲駭)計畫 105 年開 始，結合學界教師及業師共同指導具潛力且對資安精進學 習有興趣的大專及高中職學生，培訓期 1 年。已取得證書 137 人次，目前第 4 屆，培訓中學生有 108 位(含 18 名高中 職生)。 P25

	….配合資安管理法對 A、B、C 級公務機關之資安職能證書張數之 需求，107 至 108 年完成 8 個訓練機構(文化、健行、逢甲、崑 山、元智、中興、朝陽、靜宜)遴選作業，並辦理 12 門資安職 能課程訓練，計 65 班次，培訓 1,491 人次，其中 1,006 人次 通過評量取得資安職能證書…. 這些較高階之學員更可能是本資安卓越中心未來參與的人力來源。
（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）__吳嘉麗_____	

四、風險管理評估檢視表

【第一部分】：計畫現有風險圖像

嚴重 (3)			
中度 (2)		1、3	
輕微 (1)		2、4	
影響程度 可能性	不太可能 (1)	可能 (2)	非常可能 (3)

【第二部分】：計畫風險評估及處理彙總表

風險項目	風險情境	現有 風險對策	可能影響層面	現有風險等級		現有 風險值 (R)= (L)x(I)	新增 風險對策	殘餘風險等級		殘餘 風險值 (R)= (L)x(I)
				可能性 (L)	影響 程度(I)			可能性 (L)	影響 程度(I)	
1 資安卓越中心未及成立	資安卓越中心因立法或行政程序問題無法於預期時程成立	積極辦理數位發展部與其所屬資安卓越中心掛牌成立	期程	2	2	4	密切與相關部會合作協商以妥善安排後續業務交接與銜接方案。	2	1	2
2 無法招聘到足額人員	無法招聘到足額人員辦理資安卓越中心業務	以資安卓越中心可提供之國外訓練進修機會、穩定健全的工作環境、民間無法接觸到的資料研究或場域作業等為誘因吸引人才	人力	2	1	2	-	2	1	2
3 招標工期延後	近年國際COVID-19	儘可能提早辦理招標程序以	期程 經費	2	2	4	要求廠商競標	1	2	2

風險項目	風險情境	現有 風險對策	可能影響層面	現有風險等級		現有 風險值 (R)= (L)x(I)	新增 風險對策	殘餘風險等級		殘餘 風險值 (R)= (L)x(I)
				可能性 (L)	影響 程度(I)			可能性 (L)	影響 程度(I)	
	疫情嚴峻，恐造成部分採購設備因通路受阻無法進口	減少工期延後造成之影響					時提出有效之工期管理辦法			
4 無法召開國際會議或招收國際學員	因國際COVID-19疫情影響無法召開國際研討會或招收國際學員	以線上會議及課程方式替代	成效	2	1	2	-	2	1	2

【第三部分】：計畫殘餘風險圖像

嚴重 (3)			
中度 (2)	3		
輕微 (1)		1、2、4	
影響程度 可能性	不太可能 (1)	可能 (2)	非常可能 (3)

極度風險：0 項(0%)

高度風險：0 項(0%)

中度風險：0 項(0%)

低度風險：4 項(100%)

五、政府科技發展計畫審查意見回復表(A008)

審議編號：114-5010-09-20-01

計畫名稱：臺灣資安卓越深耕-資安卓越中心計畫

申請機關(單位)：數位發展部資通安全署

序號	審查意見	回復說明	修正頁碼
1	(審查委員)(最終審查意見) 本計畫以「成為亞太高階資安人才及技術創新基地」為目標，設立資安卓越中心，從資安前瞻研究、頂尖實戰人才養成、實習場域建置、國際合作及技術移轉創新育成等5個面向著手，挹注充足教學及研究資源，以厚植我國頂尖實戰人才培訓及資安前瞻研究能量，符合政策需要。惟行政法人資安研究院已成立，不再有設立資安卓越中心目標，本計畫卻未能調整計畫政策要求，需有補充說明。	謝謝委員建議，本計畫於112年國家資通安全研究院(以下稱資安院)掛牌成立並承接執行本計畫後，資安卓越中心業務亦整併於資安院組織並持續運作中，惟本計畫全程期間為 110 年至114年，於計畫啟動時尚未設立資安卓越中心，為能呈現規劃推動本計畫始末全貌之考量，故未調整計畫整體架構。 惟因應資安卓越中心已成立，有關資安卓越中心成立之詳細說明補充於計畫書P.13-P.14，相關文字亦配合調修，以避免混淆。	P.2 P.13-P.14 P.36
2	(審查委員) 本計畫所規畫目標基本上延續前期計畫持續拓展，與前期計畫規劃精神扣合，如工控場域培訓高階學員達15人、邀請國外資安學界、業界和社群知名人士結合工控場域培訓國內及國際實戰人才至少 60 人。以數量而言，相較前期成果，已有提高。惟如何認定其培訓成效及培訓人才出口，建議應予說明，以符合此成果之原始目標。	1. 為能確實發揮資安實戰人才培訓實質成效，避免流於形式上的數字績效，本計畫持續調查並規劃契合國內各界資安實戰技術之需求，受訓對象以具資安實務職場經驗之現職政府單位資安技術人員、企業資安技術人員、資安公司研發人員為主，以滿足學界、業界、政府各界需求為導向，培訓具有專業實戰技術與國際競爭力之資安菁英人才為目標，期能強化國	

	(最終審查意見) 對於培訓成效及培訓人才出口，係以問卷調查方式進行，其調查結果是否顯示人才目標有效達成，以及如何據以調整後續執行，應該加強說明	內整體資安防護能量。 2. 113 年針對進修與職涯發展產出調查問卷，針對 112 年參加過培訓課程及過往計畫之培訓課程的學員進行職涯流向調查，目的在瞭解學員的就職情形、對於課程的建議、在資安產業或關鍵基礎設施資安社群中的技術與人才貢獻等面向。透過問卷調查掌握學員的職涯現況、學員對於課程的需求建議及經驗分享，分析評估過去課程對於學員職業發展的關聯性、如何助益學員習得實務所需的專業技能等等，預期分析結果可協助未來更精確規劃培訓內容，建構符合實務資安人才所需之課程，實現培養頂尖實戰人才目標。	
3	(審查委員)(最終審查意見) 本計畫所擬定之關鍵成果與目標扣合度高，惟成果大多以執行指標件數、人次等展現，不易評估其執行品質。建議本計畫增加執行效益於預期關鍵成果中，以利展現推動成果與亮點。特別是本計畫技術成果之“卓越”性。有關研究成果卓越性的說明與實績，有必要務實納入計畫成果報告。	感謝委員建議，本計畫最終目標分別為解決國內高階資安人才不足的問題，以及成為技術創新基地，有關計畫研究成果與實績，將詳實盤點並具體呈現於計畫成果報告中。計畫目前為止執行效益說明如下： 1. 培訓符合實務資安需求之高階人才： (1) 持續調查剖析國內資安人才缺口類別及技術需求，規劃開設符	

		合國內各界資安所需之資安菁英人才課程，邀約國際資安社群講師傳授分享國際即時資安技能新知，學員包含具資安實務職場經驗之政府、企業現職資安技術人員及資安公司研發人員，並結合工控場域實際操作、雲端等新興議題，培訓具有專業實戰技術與國際競爭力之資安菁英人才。 (2)此外，更以國際資安賽事-世界駭客大賽(DEF CON CTF)為目標進行資安實戰培訓，培植更多年輕學子踏入資安領域,112年計畫協助臺灣聯隊TWN48參加DEF CON 31決賽榮獲全球第3名之殊榮，113年亦持續協助國內頂尖資安好手參加DEF CON 32，於賽前辦理賽事培訓相關活動，邀請歷屆參賽隊員提供技術指導、備戰策略、賽況模擬等，並協助選手參賽之行政資源，讓選手能專心投入賽事。目前已獲得進入決賽資格，將於113年8月赴美國爭	

		取佳績，透過推動參與國際資安大型競賽，讓我國資安年輕好手吸取實戰經驗。 (3) 本計畫並積極投入心力為培育在學及在職資安人才，培訓具有專業實戰技術與國際競爭力之資安菁英人才，進一步提升臺灣在國際上的能見度及整體競爭力。 2.研發技術成果卓越性： 前瞻研究主軸著重實務層面之應用研究，涵蓋資安重要議題，力圖將資安技術之研究成果與資安產業及關鍵基礎設施資安社群之實務需求結合，解決可能衍生之資安危害，亦為相關政策制定提供實證之基礎。目前計畫研究重點成果主要為後量子密碼演算法開發驗證以及網路訊息真實性偵測： (1)後量子密碼演算法開發驗證： a. 後量子密碼演算法驗證方法研究具有重要戰略意義，NIST 於 2023 年尚未確立後量子標準，且進入技術門檻高，產業投入重心較少，但可預期未來數年對全球網路資訊、隱私安全性造成不可控之	

		危害。爰本計畫將研究成果公開於論文及開源原始碼形式，不僅有助於擴大學術界與業界對於後量子密碼學了解與應用，還能為資安社群提供寶貴的研究基礎與工具。同時積極參與「台灣產業量子安全遷移計畫」，此計畫之合作單位包含產業署、工研院、QSMC等，並負責後量子實驗室、後量子函數庫實作的正確性、合規性與部分安全性、後量子密碼實作優化研究、量子安全教育人才培育及建立教材與教案等項目，以提早因應可預期之資安威脅。 b. 本計畫目前已開發 2 套密碼實作驗證工具，且與德國著名之安全及隱私研究所簽訂MOU，於資助計畫中決議採用其中一項驗證工具，並共同研議工具整合，以提升我國後量子密碼實作驗證結果於國際學術領域之可信度。 (2)網路訊息真實性偵測： a. 隨著科技發展速度加遽，衍生而來偽造之各	

		種網路不實輿論、詐騙訊息層出不窮，如何從大量的網路訊息中鑑識真偽已是當今各界不容忽視的社會議題，亦為國內警政單位關注之焦點。 b. 本計畫針對當今網路數據分析與網路訊息真實性辨識進行相關技術研究，協助識別和遏制散播虛假資訊的行為，目前此研發技術已有 10 多個警政及媒體相關機關機構試用，並與其中 3 家洽談授權合約，期保媒體內容的真實性與可信度，進一步對業界之資安防護有所貢獻。	
4	(審查委員)(最終審查意見) 本計畫宜有研發成果流向或串接之系統性規劃與運作，以利成果活化與反饋，加速政策目標之達成。本計畫所研發之前瞻技術宜有技術研發或產業需求之Benchmark，以印證所研發技術位居國際之領先群，亦有必要務實回覆與補強說明。	1. 謝謝委員建議，本計畫為務實解決近年可能面臨之資安威脅，偕同法人機構持續進行前瞻技術研究，並於114年將前幾年研發之技術成果落地應用。為求研發成果能滿足實務上的需求，本計畫藉由各種管道或資源執行持續與國內外專家學者交流合作，以保研發技術成果與國際接軌、甚至領先國際。 2. 團隊持續積極參與國際會議、投搞國際期刊研討會，並與國外機構、學校	

		簽訂 MOU，建立實質合作管道，蒐整掌握國際資安發展、政策趨勢及需求。而本計畫資安前瞻研究扣合國家資通安全發展方案之策略一，現下為擘劃新一階段國家資通安全發展方案，本署亦於 113 年初邀集相關部會及專家學者辦理多場訪談及座談會議，共同就國內外新型態資安威脅、資通安全前瞻科技相關研究及應用及防護技術等議題交換意見。另外與學研單位建立合作研發團隊，深化與學界間的交流合作，發揮技術研發實質效益。 2. 本計畫研發之技術已有重要階段性成果，並有多個國內、外單位採用，足以印證所研發技術位居國際之領先群，研發成果主要為後量子密碼演算法開發驗證以及網路訊息真實性偵測： (1)後量子密碼演算法開發驗證： a. 本計畫目前已開發 2 套密碼實作驗證工具，且與德國著名之安全及隱私研究所簽訂 MOU，於資助計畫中決議採用其中一項驗證工具，並共同研議工具整合，以提升我國後量	

		子密碼實作驗證結果於國際學術領域之可信度。 b. 本計畫同時積極參與「台灣產業量子安全遷移計畫」，合作單位有數產署、工研院、QSMC 等，負責項目包含後量子實驗室、後量子函數庫實作的正確性、合規性與部分安全性、後量子密碼實作優化研究、量子安全教育人才培育及建立教材與教案。 (2)網路訊息真實性偵測： a. 現今各種網路不實輿論、詐騙訊息層出不窮，已是當今各界不容忽視的社會議題，亦為國內警政單位關注之焦點。本計畫針對當今網路數據分析與網路訊息真實性辨識進行相關技術研究，協助識別資訊真偽，並遏制散播虛假資訊的行為，期保媒體內容的真實性與可信度，進一步對業界之資安防護有所貢獻。 b. 目前此研發技術已有自由亞洲電台、公共電視、天下雜誌、中央通訊社、時報資訊、鏡周	

		刊、國家安全局安全作業中心、內政部刑事警察局科技犯罪防制中心、LINE、MOMO 及國家安全局安全作業中心、內政部刑事警察局科技犯罪防制中心及事實查核中心等警政及媒體相關機關團體試用，同時授權予自由亞洲電台、事實查核中心及法務部調查局，以擴散技術能量及影響力。	
6	(審查委員)(最終審查意見) 本計畫前期審查意見多年未見處理，未見持續精進。另外本計畫已執行多年，主要場域已經建置，政府開放場域已無新指標；最後一年應總結5年計畫作為，是否達成「成為亞太高階資安人才及技術創新基地」目標有待評估、後續規劃則有待補強。	(1)本計畫全程最終目標為成為亞太高階資安人才及技術創新基地，計畫規劃分年推動資安前瞻研究、頂尖實戰人才養成、工控場域建置、跨國合作等項目，皆為達成最終目標之過程。惟全程計畫核定時期程調整至114年8月，且經費不變，囿於經費及時程因素，已無訂定工控場域建置及政府開放場域新指標，114 年關鍵成果將著重於持續培訓資安人才，及資安技術應用成果落地。為彰顯各項工作於最後一年推動之成果，確實扣合本計畫成為亞太	

		高階資安人才及技術創新基地之精神，將於114年之績效報告中總結計畫5年來各項作為之具體綜效。另為能於計畫結束後仍延續先期成果之效益，已著手規劃後續工作，並說明如下： (2)114 年關鍵成果一部分著重於持續高階學員、實戰資安人才之培訓，從根本浥注資安領域亟待補充之頂尖實戰人才。目前已規劃俟計畫結束後，將由本署另一支科技計畫「深化資安跨域整合聯防計畫」銜接，主要以培訓資安法納管機關之實戰資安人才為目標，補充政府機關資安人才缺口；另一工項則是於參與國際賽事期間(如DEF CON等)辦理團隊凝聚活動，協助提供選手討論戰略、賽況模擬等相關資源，讓選手能專心投入賽事，持續在國際資安賽事上發光。 (3)另一關鍵成果則將計畫多年研發之資安技術應用成果落地，包含完成專利2件以及	

		完成技術移轉2件，目前計畫研發網路訊息真實性辨識之成果，已著手與3家單位進行之技術移轉作業中，並未將因計畫結束而中斷，仍積極拓展技術研發成果後續的影響力。 2. 而工控場域建置及政府開放場域雖已完成階段性任務，但其運作機制及其效益並未就此中斷，計畫建置完成之工控實習場域，後續規劃將實習場域移交給該關鍵基礎設施提供者，善用既有工控模擬環境辦理資安演練、訓練符合該領域所需資安實戰人才，作為該領域資安實務人才生態之實訓場域。另政府開放場域於112年底完成環境建置與場域營運制度相關文件，產學單位可提出研究申請，113年起除維持場域運作，亦規劃提升場域資料量能，期能未來吸引更多單位申請使用，進行資安分析與防護技術之實務研究。	
7	（主計總處） 本計畫主要係延續前期設立資安卓越中心所需之人事及維運經費。114年度經費需求1億5,800萬元，較	感謝委員支持。	

	113 年度減少 1 億 7,200 萬元，係辦理資安前瞻研究、實習場域建置及資安人才養成等，考量本計畫有助於解決國內高階人才不足問題，為應其業務實際需要，建議如數照列。		
8	(數發部資安署) 依據行政院訂頒「資安產業發展行動計畫」，各政府機關之中長程個案計畫應提撥一定比例經費辦理資安防護作業(計畫經費10億以上，提撥比例為5%)；查本計畫資安經費提撥比例100%，投入項目尚屬合理，符前揭資源投入要求。	感謝委員支持。	
9	(國科會科技辦) 1. 扣合資安產業發展行動計畫(107-114 年)及六大核心戰略產業推動方案之進行前瞻資安研究、國際合作、建立需求導向之資安人才培訓體系等政策。 2. (1)計畫核心目標：持續擴大工控場域攻防技術能量、推動本國資安高等研究成果落地、持續擴大國內頂尖實戰資安人才培訓能量，符合政策目標。 (2)目標達成情形：完成期刊論文 1 篇、研討	謝謝委員建議及支持，本計畫全程目標包含資安前瞻研究、頂尖實戰人才養成、工控場域建置、跨國合作等作為，計畫推動相關作為之同時，亦有考量後續發展之實質成效，以彰顯各項成果之價值，並於114年之績效報告中呈現計畫全程各項作為之具體推動成效。目前相關成果後續發展分述如下： 1. 人才培訓學員追蹤：113年預計針對前一年度培訓之學員進行流向調查，以評估課程實訓對於學員職業發展的影響，以及對資安業界或關鍵基礎設施資安社群之技術及	

	會論文 5 篇和技術論文 3 篇，共 9 篇論文報告；完成開放工控資安之實戰課程訓練教材 1 套；組成國家資安聯隊 TWN48，參加2023世界駭客大賽(DEFCON)搶旗攻防賽(CTF)獲得全球第三名；完成醫療資安防護解決方案實證場域建置(臺北醫學大學偕同附屬醫院)，舉辦工控資安實戰課程，計 39 位學員取得證書；完成對接國外頂級資安技術或研究機構共計 5 家，並與立陶宛創新局、美加州大學柏克萊分校、德國馬克斯·普朗克安全與隱私研究所簽署合作備忘錄。 3. 本(114)年度計畫為全程計畫期程之最後一年，建議對各項成果之後續發展及進程進行追蹤分析，例如人才培訓學員之就業就職情形；工控場域之使用及擴充情形；簽署合作備忘錄後續之合作成果等。	人才貢獻度，據以進一步精進和完善課程設計。 2. 工控場域使用：本計畫評估各關鍵基礎設施人才需求之迫切性、需求性等，每年建置一座工控場域，並辦理資安實戰培訓課程，未來主要作為教育訓練及攻防演練所需。此外，111 年建置水資源工控場域作為112年跨國攻防演練(CODE 2023)場域，112 年建置醫療工控場域將規劃作為114年跨國網路攻防演練(CODE 2025)場域。後續會將場域移交給所屬關鍵基礎設施提供者，期善用既有工控模擬環境辦理該領域所需之資安相關演練。 3. 國際合作：積極與已簽屬 MOU 之產學界研究機構緊密交流洽談實質合作，包含： (1)110 年與加州大學柏克萊分校長期網路安全研究中心(CLTC)簽訂 MOU，111 年推動「2030 網路安全展望」台灣站以及台灣學者短期移地研究等項目，112 年推動「資安人才培育及資安意識推廣經驗、教材及工具」與「AI 安全政策及國際 AI 相關法規」等項目，與 CLTC 建立長期合作架構，進行資訊交流分享及相關研究	

		合作，113 年雙方亦先後相互到訪持續進行 AI、資安法規等各類相關新興議題進行交流。 (2)111 年與日本情報通信研究機構(NICT)開啟雙邊合作，連續 2 年邀請 NICT SecHack365 校友隊參與網路威脅防禦競賽，112 年共同辦理「TWN-NICT Cybersecurity Workshop」，資安技術及相關應用研發進行交流與合作討論，擴增我國資安人培之國際視野。 (3)111 年與德國馬克斯普朗克安全及隱私研究所(MPI-SP)簽訂 MOU，建立長期合作架構，可共同開發技術，瞭解他國資安領域發展。112 年本計畫開發後量子加密驗證工具 CryptoLine，已被 MPI-SP 資助之 Formosa Crypto 計畫決議採用，並邀請我方研究人員分別於參與會議共同討論工具整合。	
10	(會議審查綜合意見) 請於計畫書內容補充說明事項：是否成立資安卓越中心。	本計畫全程期間為 110 年 1 月 1 日至 114 年 8 月 31 日，110 年至 111 年原由國家實驗研究院執行，110 年即分別於臺北及臺南完成設置資安卓越中心辦公室。俟 112 年國家資通安全研究院(以下稱資安院)掛牌成立並承接執行本計畫後，資安卓越中心業務亦整併於資	P.2 P.13-P.14 P.36

		安院組織並持續運作中，有關資安卓越中心成立之詳細說明補充於計畫書 P.13-P.14。	

註：主筆委員完成審查意見後，系統將主動發信通知，請於期限前至「政府科技計畫資訊網」填寫完成意見回復。

六、資安經費投入自評表(A010)

(如有填寫疑問，請逕洽行政院資安處 3356-8063)

部會	數位發展部		單位	資通安全署			
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
114-5010-09-20-01	臺灣資安卓越深耕-資安卓越中心計畫	5	1,617,000	1,617,000	1,617,000	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	2-3(C2、C3)	頂尖實戰人才培訓及資安前瞻研究	409,000
2	111	2-3(C2、C3)	頂尖實戰人才培訓及資安前瞻研究	400,000
3	112	2-3(C2、C3)	頂尖實戰人才培訓及資安前瞻研究	320,000
4	113	2-3(C2、C3)	頂尖實戰人才培訓及資安前瞻研究	330,000
5	114	2-3(C2、C3)	頂尖實戰人才培訓及資安前瞻研究	158,000
總計				1,617,000

備註：

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

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

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

2、 投入項目類別請用下列代號填寫：

2-1 系統開發

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

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

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

2-2 軟硬體採購

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

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

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

2-3 其他建議項目

(C1) 資安檢測標準研訂。

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

(C3) 新興資安領域之人才培育。

（C4） 編撰資安訓練教材。

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

七、其他補充資料

無。