中　華　民　國　116　年　度

數位發展部監督

國家資通安全研究院預算

國家資通安全研究院 編

國家資通安全研究院

目次

中華民國 116 年度

總說明

國家資通安全研究院

總說明

中華民國 116 年度

一、概況

(一)設立依據

國家資通安全研究院(以下簡稱本院)設置條例經總統 111 年 1 月 19 日華總一義字第 11100003351 號令公布，行政院核定 112 年 1 月 1 日施行。

(二)設立宗旨

國家資通安全研究院（以下簡稱本院）依據《國家資通安全研究院設置條例》設立，係國家推動資通安全政策、強化數位治理及提升整體防護韌性之專業行政法人。本院配合國家安全、數位發展及資通安全政策方向，擔任政府資通安全技術幕僚與防護支援角色，協助建構完善之國家資通安全治理體系，提升政府機關、關鍵基礎設施及整體社會因應資安風險與重大事件之能力，確保國家數位環境安全、穩定及可信。

隨著數位轉型持續深化，人工智慧、雲端運算、物聯網及各類新興科技廣泛應用，政府服務、產業運作及民生基礎設施對數位系統依賴日益提高；另一方面，國際資安威脅、供應鏈風險、組織型駭侵及跨境網路攻擊亦呈現複雜化、常態化及高度不確定性。資通安全已不僅為資訊技術或內部管理議題，更涉及國家安全、政府持續運作、社會秩序維護、產業穩定及人民權益保障，爰有必要建立具前瞻性、整合性及持續性之國家級資安專業支援機制。

本院以維護國家資通安全、強化數位韌性及支援政府決策為核心使命，持續協助研析國內外資安情勢與新興風險，支援國家資安政策、制度及防護機制之規劃與推動；並強化政府機關及關鍵基礎設施之資安治理、威脅預警、技術檢測、事件通報、鑑識分析、應變處置及復原協處能力，深化跨機關、跨領域之情資共享與聯防合作，提升重大資安事件

之整體應處效能。

面對人工智慧安全、零信任架構、資料保護、數位訊息威脅、產品與供應鏈安全及工業控制系統防護等重要議題，本院將持續整合政策、技術、治理、應變及人才等專業能量，強化風險辨識、主動防禦及制度支援，並深化與國際資安組織及理念相近國家之合作交流，掌握全球資安政策與技術發展趨勢，提升我國國際參與及跨境聯防能力。

未來，本院將秉持專業、客觀、前瞻及協作原則，持續發揮國家級資安專業機構功能，支援政府完善資安治理、提升技術自主及防護量能，厚植全民資安意識與專業人才基礎，並促進政府、產業及社會共同承擔資安責任，以維護國家安全、保障人民權益及支撐數位經濟穩健發展，逐步建構安全、可信且具韌性之數位國家。

- 本院業務範圍包含：
  1. 研發資通安全科技，推動資通安全技術應用、移轉、產學服務及國際交流合作。
  2. 協助規劃及推動國家資通安全防護機制。
  3. 協助政府機關(構)及關鍵基礎設施重大資通安全事件應變處置。
  4. 協助規劃及支援國家關鍵基礎設施之資通安全防護。
  5. 協助規劃及培育資通安全專業人才；推廣全民資通安全意識。
  6. 支援具有特殊敏感性之政府機關(構)資通安全防護工作。
  7. 支援產業資通安全重大發展及法規推動之需求。
  8. 其他與資通安全科技相關之業務。
- 本院經費來源：
  1. 政府之核撥及捐(補)助。
  2. 國內外公私立機構、團體及個人之捐贈。
  3. 受託研究及提供服務之收入。
  4. 其他收入。

(三)組織概況

本院組織架構以強化國家資通安全防護、資安人才培力及資安關鍵技術發展等功能角色，在技術面包含檢測防禦、威脅分析及通報應變等 3 個中心，管理面包含前瞻研究籌獲、國際合作及資安治理、人才培力等 3 個中心，據以銜接國家政策推動與本院業務範圍，並由綜合管理處擔任行政支援角色，本院組織圖詳見圖 1。

本院監督機關為數位發展部，設有董事會，並置監事 3~5 人，分別行使監督與查核等職權。本院設有院長 1 人，由董事長提請董事會通過後聘任之，負責本院營運及管理業務之執行，並設副院長 2~3 人，輔佐院長襄理本院業務，另下設稽核室，規劃推動內部稽核業務。

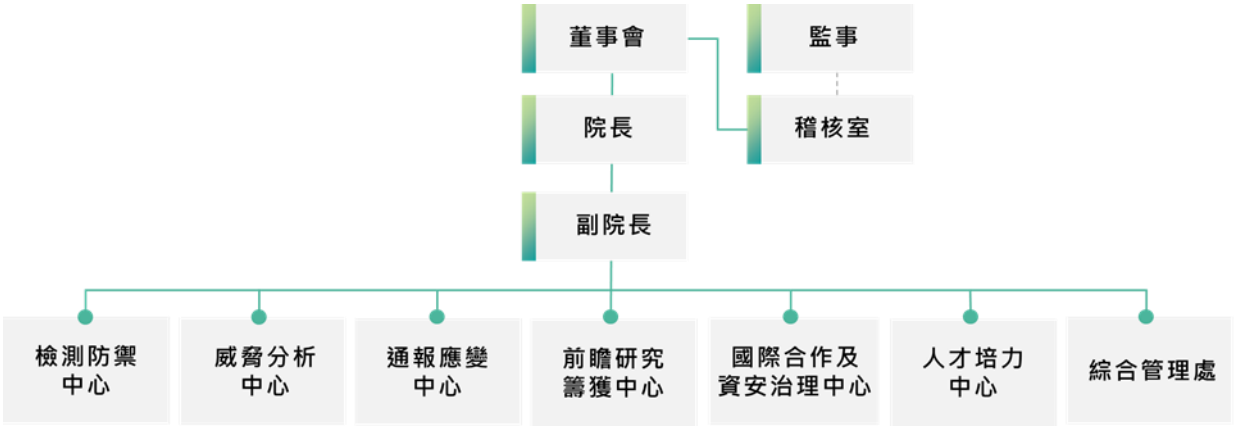


圖 1 國家資通安全研究院組織圖

本院檢測防禦中心、威脅分析中心、通報應變中心、前瞻研究籌獲中心、國際合作及資安治理中心、人才培力中心、綜合管理處之職掌，詳見表 1。

表1　國家資通安全研究院各單位職掌

單位	職掌
檢測防禦中心	▪政府組態基準規劃及執行 ▪資安弱點通報機制規劃及執行 ▪資通系統滲透測試 ▪資通安全管理法相關技術檢測服務 ▪主動防制機制規劃及技術研發

單位	職掌
	▪工業控制系統資安檢測技術研發 ▪資安模擬場域規劃及建置 ▪共用資通安全系統開發及維運 ▪其他有關資安檢測防禦事項
威脅分析中心	▪網路威脅情蒐與攻擊趨勢分析及預警 ▪社交工程攻擊情蒐機制規劃及執行 ▪政府骨幹網路情資蒐集及分析 ▪政府聯防情資蒐集、分析與聯防 ▪資安情資整合及分享 ▪各項情資威脅技術研究及應用 ▪其他有關資安威脅分析事項
通報應變中心	▪資安監控及警戒服務 ▪資安事件通報諮詢 ▪資安事件鑑識分析 ▪政府機關與關鍵基礎設施重大資安事件應變協處 ▪組織型駭侵研究 ▪端點偵測及回應機制規劃及執行 ▪其他有關資安通報應變事項
前瞻研究籌獲中心	▪新興資通訊資安防護需求研析及規劃 ▪產學研合作研究規劃及推動 ▪新興資安應用技術發展研析 ▪新興資安技術規範與基準研訂 ▪資安應用科技研究及技術開發 ▪資安防護應用技術研究及移轉 ▪數位訊息防護應用技術研究及移轉 ▪資安韌性巡檢服務 ▪其他有關前瞻資安技術研究籌獲事項
國際合作及資安治理中心	▪國家資通安全策略研析 ▪資安研究國際合作及情資分享

單位	職掌
	▪ 國際資安攻防協作 ▪ 國際資安人才合作培育 ▪ 資安國際情勢觀測及研析 ▪ 關鍵基礎設施資安防護研析 ▪ 資安標準與規範研析 ▪ 其他有關國際合作及資安治理事項
人才培力中心	▪ 資安人才職能發展框架及評量機制研析與推廣 ▪ 資安人才培訓課程規劃及開發 ▪ 關鍵基礎設施培訓課程開發及維護 ▪ 資安實戰課程開發及維護 ▪ 資安認知意識與防護實務推廣 ▪ 其他有關資安人才培育事項
綜合管理處	▪ 組織人事、採購、文書、印信、出納、財產及總務等業務規劃、推動與營運管理相關事項 ▪ 人力資源規劃管理與執行 ▪ 組織財務整體規劃，包含年度收支預、決算之籌劃，預算管控，財務規劃擬定 ▪ 計畫之規劃、審查、管制考核及績效評鑑 ▪ 計畫管理運作相關制度與程序之建置及組織發展規劃 ▪ 組織各項資訊作業與網站之規劃、維護、管理及整體資訊系統維運管理與各類資訊應用支援 ▪ 民意機關、新聞媒體間聯繫及服務業務辦理 ▪ 全院法制業務及涉訟案件處理 ▪ 其他有關綜合管理業務

二、前年度執行成果概述

114 年度重點工作項目之年度目標與執行成果，詳見表 2。

表2　114 年計畫執行成果

工作項目	年度目標	執行成果
培育資安人才	▪邀請國外資安學界、業界及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	▪培育 97 名學員結業，其中包含 85 名企業與資安公司之技術實務人員
推動公私協同治理	▪因應國際資安威脅趨勢及新興科技發展，並參照資安規範整體發展藍圖增修參考指引 ▪提供 10 個政府機關資安技術檢測服務 ▪每稽核場次支援 1 位稽核委員 ▪對接國外頂級資安技術或研究機構至少 1 家以上 ▪發行資通安全技術年報 ▪完成 1 場關鍵基礎設施領域跨國攻防演練 ▪促進各 CI 領域優化其風險情境評估結果，完成我國資安風險地圖 ▪研析並提出資通安全管理法之發展建議	▪完成 3 項資安參考指引之修訂與發布，涵蓋資通系統風險評鑑、無線網路安全及電腦機房異地備援等資安領域。提升政府機關風險評鑑能力，以及強化無線網路及電腦機房異地備援管理之指引 ▪完成 10 個政府機關資安技術檢測服務 ▪配合資安署之資安實地稽核規劃，全年共計支援 40 人次 ▪與澳洲昆士蘭大學簽屬合作備忘錄共計 1 份 ▪完成資通安全技術年報 ▪完成 1 場緊急救援與醫療領域跨國攻防演練，共 12 隊紅隊與 4 隊藍隊參與 ▪「促進各 CI 領域優化其風險情境評估結果，完成我國資安風險地圖」及「研析並提出資通安全管理法之發展建議」」，因配合政策及預算調整，故刪減此項目標，異動說明詳註 1
政府網路資安縱深防護	▪完成 1 場至少 70 個政府機關之網路攻防演練	▪完成 71 個政府機關 2 階段社交工程演練與 1 場資通系統實兵演練

工作項目	年度目標	執行成果
	▪建置 1 個關鍵基礎設施攻防演練場域 ▪產出 2 則組織型駭侵偵測規則 ▪協助資安法納管機關資安事件通報作業並提供諮詢服務 ▪協助機關提出技術支援之事件鑑識與分析作業 ▪彙整 A、B 級公務機關之 EDR 事件資料並進行關聯分析 ▪成立至少 2 件警戒專案，完成專案報告 ▪執行 6 個重點機關 7x24 資安監控作業 ▪強化推動 A 級公務機關導入黑名單自動化部署服務 ▪新增收容 2 種國際資安威脅指標，強化情資分享內容 ▪完成零信網路導入與研析執行報告 ▪協助 A 級公務機關完成核心網通設備導入資通安全弱點通報機制	▪完成建置緊急救援與醫療領域攻防演練場域 ▪產出 5 則組織型駭侵偵測規則 ▪總計接獲 1,303 件資安事件通報，並提供 1,837 件通報諮詢服務 ▪成立 2 件通報事件處理案協助機關進行調查；同時因應特定專案、追查駭客所控之中繼站，成立 3 件專案事件處理案 ▪接收 41 件 EDR 事件單，分析對應樣本 81 個，共計 8 種樣本分類 ▪完成 9 件警戒專案之專案報告 ▪執行 6 個重點機關 7x24 資安監控作業 ▪114 年 7 月 21 日辦理黑名單自動化部署服務說明會。累積共 185 個機關完成導入，其中包含 39 個 A 級公務機關 ▪「完成零信網路導入與研析執行報告」因配合政策及預算調整，故刪減此項目標，異動說明詳註 1；然 114 年完成協助 3 個中央 B 級機關零信任架構身分與設備鑑別導入作業並完成結案報告 ▪「協助 A 級公務機關完成核心網通設備導入資通安全弱點通報機制」因配合政策及預算調整，故刪減此項目標，異動說明詳註 1

工作項目	年度目標	執行成果
技術基準研究	▪研究 2 項安全組態基準與部署方式 ▪檢討與精進政府組態基準發展項目 ▪製作安全組態基準實作文件與數位影片 ▪推動至少 1 項技術移轉或採用案例 ▪完成 2 個重大弱點研析	▪完成 4 項安全組態基準與部署方式 ▪完成 5 項政府組態基準檢討與精進 ▪完成 2 項實作文件與數位影片 ▪推動技術移轉 114 年新案:內政部移民署、外交部領事事務局、法務部司法官學院；114 年延續案:法務部調查局、財團法人新北市台灣事實查核教育基金會 ▪完成 PHP-CGI(CVE-2024-4577)與 Apache Tomcat(CVE-2025-24813)漏洞之成因分析與實作驗證
強化委外風險管理	▪辦理 10 個機關資安防護輔導服務 ▪檢視 5 份現行共同供應契約規範 ▪辦理現行 5 類資安服務廠商評鑑作業	▪完成 20 個機關資安防護輔導服務 ▪完成 6 類資安服務之採購規範之修訂 ▪完成現行 5 類資安服務廠商評鑑作業
推動資安技術 AI 化	▪開發威脅態勢預警技術 1 式 ▪開發攻擊酬載來源鑑別技術 1 式 ▪開發未知漏洞風險識別技術 1 式 ▪開發 AI 主動戰情匯流追跡技術 1 式	▪114 年配合計畫預算刪減，調整工項為 2 項(開發威脅態勢預警技術 1 式、開發攻擊酬載來源鑑別技術 1 式)

工作項目	年度目標	執行成果
推動 AI 網路主動防禦研發生態系之友善環境	▪提供 AI 應用政策、治理等相關基準研析或推動建議報告至少 3 篇 ▪提供應用 AI 於網路主動防禦相關教材 1 式 ▪辦理 AI 網路主動防禦技術/情報交流會至少 2 場	▪本工作項目「推動 AI 網路主動防禦研發生態系之友善環境」因配合政策及預算調整，故刪減本工項之年度目標，異動說明詳註 1
強化台灣電腦網路危機處理暨協調中心(TWCERT/CC)	▪受理與審核國內企業產品資安漏洞通報至少 30 個 ▪接收民間企業事件通報，提供技術諮詢服務 ▪完成每月發布之資安電子報 ▪參與 3 場國際資安組織活動或國際大型資安研討會議 ▪完成每月蒐整上市櫃公司資安事件概況 ▪掌握供應鏈攻擊廠商，追蹤修補進度	▪共有 52 個弱點等級達 9 以上之產品，發布情資通知 15 個單位 ▪接收民間企業事件通報，提供技術諮詢服務 ▪完成 12 份每月資安電子報發布 ▪出席 3 場指標性國際資安年會(APCERT、FIRST 及 CERT-EU)，即時掌握最新 AI 攻防、事件應變自動化及資安治理趨勢，促進國內技術方向與國際接軌 ▪蒐集資安重訊概況，114 年總計發布 76 件重訊，依市場別統計以上市公司發布最多
協助維運資安管理相關資通訊系統	▪維運 16 個資安署委託代管之資通系統	▪完成 16 個資安署委託代管之資通系統之全年維運與資安防護作業，包含 2 個核心系統與 14 個非核心系統
辦理政府韌性系統服務工作執行計畫	▪整備(新增或更新)30 項軟體模組物件 ▪盤點民生關鍵資訊系統背景資料 20 項	▪完成整備(新增或更新)30 項軟體模組物件 ▪完成盤點民生關鍵資訊系統背景資料 22 項

工作項目	年度目標	執行成果
	▪完成數位韌性領航員訓練課程至少 10 名(含複訓) ▪完成 6 項民生關鍵資訊系統以及 33 項機關業務運作系統之巡航作業，並提供技術輔導與執行改善複審作業 ▪完成資訊專案文件與開源碼詮釋資料中文化 5 案 ▪調校(新增與編修)政府系統設計元件 10 案	▪完成數位韌性領航員訓練課程 12 名(含複訓) ▪完成 22 項民生關鍵資訊系統以及 42 項機關業務運作系統之巡航作業 ▪「完成資訊專案文件與開源碼詮釋資料中文化 5 案」及「調校(新增與編修)政府系統設計元件 10 案」，因配合政策及預算調整，故刪減此項目標，異動說明詳註 1
辦理各級政府服務韌性運作與容錯環境規劃及資訊服務	▪完成 1 個 AI GSN 網路防禦策略模型 POC 驗證 ▪輔導 A 級機關導入零信任設備鑑別技術，完成 10 個機關導入 ▪完成 18 項機關業務系統之跨境公有雲資安合規技術實地輔導 ▪調查與彙整各資安 A 級機關使用零信任軟體之情形與意見回饋報告 ▪完成 1 個政府資訊防偽共通資訊平台 POC 驗證	▪完成 1 個 AI GSN 網路防禦策略模型 POC 驗證 ▪完成 10 個 A 級機關導入信任架構 ▪配合政策及預算調整，故核定補助計畫目標調整為 9 項機關業務系統，並完成 9 項機關業務系統之跨境公有雲資安合規技術實地輔導 ▪「調查與彙整各資安 A 級機關使用零信任軟體之情形與意見回饋報告」及「完成 1 個政府資訊防偽共通資訊平台 POC 驗證」，因配合政策及預算調整，故刪減此項目標，異動說明詳註 1
辦理各級政府數位服務應變與公私協力環境規	▪完成雲原生系統架構原則與服務導入文件 1 式	▪完成雲原生系統架構原則與服務導入文件 1 式

工作項目	年度目標	執行成果
劃、營運與輔導服務	▪完成 1 項 AI 模型在使用者體驗分析應用概念驗證 ▪完成 1 個 APP 無障礙驗證工具自動化架構 ▪完成數位服務設計流程指引 1 式 ▪完成 AIOps 工具或服務導入文件 1 式	▪完成 1 項 AI 模型在使用者體驗分析應用概念驗證 ▪「完成 1 個 APP 無障礙驗證工具自動化架構」、「完成數位服務設計流程指引 1 式」及「完成 AIOps 工具或服務導入文件 1 式」3 項年度目標，因配合政策及預算調整，故刪減此項目標，異動說明詳註 1
維運管理 NCCSC 平臺	▪盤點國內內陸介接站網路系統之關鍵基礎設施，建立監理、通報應處機制，完成海纜內陸介接站之設施暨服務告警收容	▪本工作項目原訂年度目標為「盤點國內內陸介接站網路系統之關鍵基礎設施，建立監理、通報應處機制，完成海纜內陸介接站之設施暨服務告警收容」因配合政策及預算調整，故計畫核定調整年度目標為「NCCSC 平臺 7*24 小時之可用性」，俾即時掌握通傳事業網路運作狀況與資安事件，確保資安事件通報應變流程管道順暢，每週定期產出「NCCSC 各通報及分享數據報表」
協助督導通傳業者落實資通訊設備 CVE 漏洞修補作業	▪納管通傳業者使用之防火牆、交換器及路由器，及時修補 CVE 漏洞	▪114 年度共通報漏洞 476 筆，協助業者進行資通設備漏洞修補作業
配合辦理 A 級機關應辦事項	▪配合辦理弱點掃描 2 次 ▪配合辦理滲透測試 1 次 ▪配合辦理資安健診 1 次 ▪配合辦理營運持續計畫演練 1 次	▪完成 2 次弱點掃描與複測修補作業 ▪完成滲透測試、資安健診、2 次內部稽核、BCP 演練、外部稽核之矯正與修補作業

工作項目	年度目標	執行成果
辦理通傳事業資安攻防演練	▪完成1場通傳事業資安攻防演練	▪完成辦理1場通傳事業資安攻防演練，參加業者共計7家，10個系統
辦理通傳事業資安教育訓練	▪辦理3場通傳事業資安防護教育訓練	▪本工作項目原訂年度目標為「辦理3場通傳事業資安防護教育訓練」因配合政策及預算調整，故計畫核定調整年度目標為「辦理2場次教育訓練」，於5月與9月辦理2場次教育訓練，並獲得98%以上參訓學員對於課程內容與規劃表示極高滿意度
辦理通傳情資分享會議	▪辦理4場通傳事業情資分享會議	▪於114年3月、6月、9月及12月，辦理4場通傳事業情資分享會議
辦理通傳領域關鍵基礎設施提供者資安稽核作業	▪辦理至少6個通傳領域關鍵基礎設施提供者資安稽核作業	▪辦理6家關鍵基礎設施提供者資安稽核作業及3家公眾電信網路設置者資安檢驗作業
發展隱私保護前瞻研究	▪開發聯合學習、同態加密通用型實作程式碼工具 ▪持續試辦技術驗測，以成熟技術驗測機制	▪完成資料保護與實用性研究報告1份 ▪完成開源工具實作1式 ▪完成國際資料保護驗測流程及制度研析1式
擴展隱私強化技術應用	▪累計完成3案概念性驗證案例，且至少一案應用新興技術聯合學習或同態加密 ▪為推廣隱私強化技術創新應用，透過參與大專院校相關競賽，並選出至少3個學生優秀作品	▪完成拓展機敏資料保護實證場域，完成1個最小可行性評估概念性驗證場域以及完成1個深化概念性驗證場域 ▪完成隱私強化技術創新應用活動規劃及辦理「大專校院資訊應用服務創新競賽(InnoServe)」，資料隱私保護

工作項目	年度目標	執行成果
		創新應用組共 9 個參賽團隊報名，最終選出前 3 名以及 2 名佳作
台灣中小微型企業及非營利組織資安現況研究	▪ 提出中小型及微型組織資安防護及輔導政策建議 ▪ 提出客製化培訓課程內容及培訓方法建議 ▪ 產出研究報告，供後續宣導及推廣使用	▪ 完成資安現況研究並轉化為培訓與輔導規劃依據，符合研究與政策建議目標
編製及推廣資安培訓及提升資安意識系列教材	▪ 開發 5 份綜合訓練教材與教案(實體或線上版)	▪ 完成開發 5 門線上課程與 5 本基礎資安實務系列手冊
提供中小企業資安服務	▪ 培訓 20 位資安實務種子師資，提供 20 個資安實地輔導以及推動資安檢視 150 個組織	▪ 完成 20 個資安實地輔導給予資安防護建議，並提供至少 224 個組織線上實體培訓
開設網路安全實務與社會課程，培訓資安輔導員	▪ 與地區 6 所大學合作，開設 6 門「網路安全實務與社會」課程 ▪ 培訓 200 位學生輔導員，提供資安輔導及諮詢服務	▪ 完成與國內 8 所大學合作開設 9 門課程，培訓至少 300 位學生輔導員提供資安諮詢
擴展提升資安意識系列活動	▪ 透過線上與線下展示及推廣活動，提供全民資安意識宣導資料，預計觸及 10,000 人次以上民眾	▪ 完成辦理資安大會、資安人培研討會等實體活動，以及線上宣導文宣，觸及 10,000 人次以上
鏈結公私部門資源協力推動	▪ 透過公私協力，與 6 個以上公私團體合作，達成本計畫輔導 3,200 家	▪ 完成與業界法人、非營利組織公益團體、大專院校等 6 個以上團體合作，運用其線上線下

工作項目	年度目標	執行成果
	以上中小微型營利/非營利組織、觸及 32,000 名以上企業員工與 18,000 以上一般民眾提升資安意識及防護之目標	實體平台，已觸及 22,788 人次，往後將持續累積與擴增
評估、威脅狩獵、事件處理及自動化研發	▪ 成立關鍵基礎設施資安防護團隊達至少 24 人 ▪ 完成標準作業程序新增與修訂 ▪ 辦理 2 處關鍵基礎設施資安防護檢測作業 ▪ 辦理國內外工控系統資通安全教育訓練至少 1 場 ▪ 辦理或參與至少 1 場國內外工作坊、論壇或是高峰會	▪ 建置檢測團隊人數達 24 人 ▪ 完成標準作業程序修訂 1 式 ▪ 完成 3 處關鍵基礎設施資安防護檢測作業 ▪ 辦理 1 場工控系統資通安全教育訓練 ▪ 辦理 1 場國內外工作坊 (Workshop)
數位靶場與資通安全桌上推演	▪ 數位靶場需求分析與架構規劃 ▪ 關鍵基礎設施資安桌上推演(Tabletop Exercise)方法論建構 ▪ 資通安全桌上推演情境 1 式	▪ 完成關鍵基礎設施數位靶場需求分析與架構規劃 ▪ 完成關鍵基礎設施資安桌上推演(Tabletop Exercise)方法論建構 ▪ 完成關鍵基礎設施資安桌上推演情境 1 式
資安治理成熟度評估機制及資通安全輔導服務	▪ 協助推動 A、B 級公務機關之 IT 資安治理成熟度持續提升	▪ A 級公務機關 IT 資安治理成熟度達 3 級以上之比例，共計 84% (41/49) ▪ B 級公務機關 IT 資安治理成熟度達 3 級以上之比例，共計 63% (140/221)

工作項目	年度目標	執行成果
	▪協助推動 A、B 級關鍵基礎設施提供者之 IT 與 OT 資安治理成熟度持續提升	▪IT 資安治理成熟度： ▪A 級 CI 提供者 IT 資安治理成熟度達 3 級以上之比例，共計 76% (28/37) ▪B 級 CI 提供者 IT 資安治理成熟度達 3 級以上之比例，共計 60% (49/81) ▪OT 資安治理成熟度： ▪A 級 CI 提供者 OT 資安治理成熟度達 3 級以上之比例，共計 59% (23/39) ▪B 級 CI 提供者 OT 資安治理成熟度達 3 級以上之比例，共計 46% (44/95)
	▪辦理 10 個機關資安防護輔導服務	▪辦理 1 梯次輔導訓練課程，20 個機關資安防護實地輔導
註：表 2 所列年度目標係依原規劃內容所訂定之預定績效指標。惟 114 年度受預算審議結果、政策優先順序調整及實際業務推動需求影響，部分計畫執行範圍與重點有所調整，致原訂年度目標與實際成果間產生差異。相關調整均係配合政策推動及資源配置之合理變動，並已在既有預算與人力條件下，優先確保關鍵資安業務之推動與整體執行效益。		

三、業務計畫

依據本院設置宗旨、業務職掌及 116 年發展藍圖，本院 116 年度將承接數位發展部及所屬機關之資通安全相關補助計畫，統籌整合各中心專業能量，推動「政府資通安全防護工作執行計畫」、「關鍵基礎設施資安防護計畫」、「AI 網路威脅偵防技術研究計畫」、「數位訊息分析技術研發計畫」、「全民資安意識與韌性延伸推動」、「提升通傳領域資安聯防機

制及強化通傳網路預警應變能力」、「資料保護驗測機制推動計畫」及「中小企業及產品資安強化計畫」等 8 項計畫。

本年度工作計畫以「強化國家資安防護與數位韌性」為核心，聚焦政府防護應變、關鍵基礎設施、AI 威脅偵防、數位訊息與情資研析、全民資安意識、通傳聯防、系統服務韌性、資料保護治理，以及產業供應鏈安全等面向。透過跨中心協作，將各項補助計畫與本院核心職掌、年度目標深度串接，構築「政策支援、技術研發、檢測防護、通報應變、治理推動、人才培育」的一體化推動架構。已爭取之政府補助計畫說明如下。

藉由上述計畫之落實，本院將有效協助政府提升資安治理成熟度、重大事件應變效率與跨域聯防效能；同時支援產業強化產品安全與供應鏈韌性，逐步擴大全社會資安防護能量，實踐國家資安政策目標，堅實支撐安全、可信且具韌性之數位國家發展。

(一)116 年政府資通安全防護工作執行計畫

1. 業務內容

本計畫旨在配合數位發展部資通安全署推動「數位政府資安生態防護推動計畫」、「政府數位韌性強化計畫」暨「國家資通安全研究院營運發展計畫」。由本院統籌整合內部六大中心業務職掌，全力支援國家資安防禦相關作業之遂行。

計畫以「強化數位政府資安韌性」為核心布局，推動國家資安防護規劃、重大資安事件應變、敏感機關資安支援、資安人才培育、政府資安治理、主動防禦及公私協力情資分享等核心工作；並透過導入零信任、關鍵基礎設施防護、攻防演練、漏洞通報及 TWCERT/CC 運作精進，用以提升政府與產業整體防護、事件應變及國際接軌能量，俾支撐安全可信智慧國家之建構。同時，本年度亦將落實進駐資安園區行政大樓北棟之各項籌備作業，以奠定本院長遠營運發展之基石。

(1) 培訓資安前瞻人才，建構完善資安人才生態系

- 推動現行資安職能基準及培訓

  配合《資通安全管理法》修正條文，研析機關資安專職人員之核心任務與職能需求，檢視「資安人才職能發展框架」妥適性、滾動修正「資安職能訓練發展藍圖」；並因應新興資安議題開發教材，建構各類資安人員之課程地圖與學習路徑，以精準契合當前資安技術與防護趨勢。另辦理認證之職能訓練機構教學查核及支援資安署所舉辦調訓等活動講師支援。

- 辦理資安技能競賽金盾獎

  為鼓勵年輕學子投入資安領域，透過競賽切磋交流，達成向下扎根與防護意識推廣之實效，賡續辦理「資安技能競賽金盾獎」。競賽題型將結合理論與實務判斷，並融入最新攻擊手法、資安風險趨勢及 AI 應用，藉以強化學生技術實力、發掘潛在人才，全面提升校園資安素養。

- 活絡國內資安賽事生態

  透過進階 CTF(Capture the Flag)實戰之漏洞挖掘、逆向工程與密碼破譯等核心技術剖析，激發入門學子之邏輯思維與解題潛力，引領新手跨越技術門檻，蛻變為具備中高階攻防實戰能量之選手；並透過新興資安職能需求分享，啟發學生對前沿技術之研究熱忱，形塑具跨域解決問題能力與國際視野之資安人才。

- 凝聚國際資安賽事團隊

  為鼓勵臺灣資安團隊積極參與國際資安賽事(如 DEFCON CTF)，提供晉級決賽團隊在職選手(上限 6 名)出國參賽補助，每位至多 15 萬元，用以支應食宿、機票及門票等相關經費，藉此引導國內優秀人才接軌國際。

(2) 強化政府資安治理，共創安全數位環境

- 零信任架構資安防護

  為落實我國關鍵基礎設施之資安防護，本工項積極推動政府機關導入零信任架構。具體作法包含蒐整國內外導入政策、技術文件與實務經驗，研擬「零信任架構導入指引」；並針對關鍵部署模式，於既有「資源門戶存取模型(Resource Portal-Based Model)」基礎上，進一步擴充研訂「裝置代理/閘道模式(Device Agent/Gateway Model)」相關參考文件，藉此帶動商用解決方案之技術成熟與完備，全面提升國家整體資安韌性。

- 編修資安參考指引

  密切掌握國際資安威脅趨勢、新興科技發展、國際標準演進及我國法制規範之修訂，定期檢視並動態調整資安相關規範之整體發展藍圖；並依據藍圖規劃時程，編撰或修訂相應之資安參考指引。

- 推動 IT 資安治理成熟度

  持續精進公務機關與 CI 提供者 IT 資安治理成熟度機制與評估問項，並協助推動 IT 資安治理成熟度評估作業，包括提供公務機關與 CI 提供者 IT 資安治理成熟度評估機制線上教學課程、提供評估問項諮詢服務及輔導等，以持續提升各公務機關與 CI 提供者之 IT 資安治理成熟度等級。

- 推動工控領域(OT)資安治理成熟度

  深化 OT 資安治理成熟度機制與評估指標，優化相關評估作業。具體作為包括提供 OT 資安治理評估機制線上課程、諮詢服務與專案輔導，戮力提升 CI 維運公務機關與 CI 提供者之 OT 資安治理成熟度等級，強化實體防禦韌性。

- 資安刊物編審與發布

落實資安週報、季報及年報之編輯、審核與發布作業。定期廣泛蒐集國內外資安威脅情資、重大資安事件、漏洞資訊及政策動態，進行深度研析與撰稿。同時嚴格把關內容編修、排版校稿與品質控管，確保依限發布並落實成果歸檔，以提供前瞻資安趨勢與重點觀察，協助相關單位精準掌握最新情勢，作為資安治理、風險管理及決策之關鍵依據。

- 國際資安政策法制觀測與研析

  鑑於技術演進與國際情勢變化迅速(如 AI 及其治理議題)，本工項將持續觀測重要國家、區域組織(如歐盟)在資安與關聯政策、法制上之應對策略及前沿辯論，俾利作為我國完善健全法制、調整國家政策及推進國際合作之參考對象。

- AI 政策法制議題研析與國際活動之參與

  – AI 政策法制議題研析

    緊密追蹤國際討論走向，精選並深入研析最新、最關鍵之 AI 政策法制議題；除針對議題本身提供核心研究洞見外，亦對其長期政策影響進行趨勢預判與前瞻因應建議。

  – AI 國際活動之參與

    透過出席國際會議、研討會及常態性交流機制，實質參與國際 AISI 網絡、重要國際組織之 AI 主題工作組，以及其他國際機構與相關社群之對話，深化我國在 AI 領域之國際能見度與鏈結度。

- 國際資安合作交流

  持續拓展與五眼聯盟、歐洲及亞太地區等理念相近國家與重要資安夥伴之實質合作，透過雙邊對話、專家交流、人員互訪、合作專案，以及線上或實體會議等多元形式，建立並深化雙邊或

多邊合作機制，並視合作議題推動資安政策、技術交流、情資分享、資安演練及共同研究等合作，強化我國跨國資安聯防與國際鏈結。

對接國際重要資安技術或研究機構，掌握國際資安政策規範、技術發展及應用趨勢，並至少新增 1 家具國家影響力或資安技術量能之國外資安機構作為合作夥伴。透過持續交流與專案洽談，引進國際資安實務經驗，作為我國推動資安政策研析、技術合作及防護能量提升之基礎。

持續深化我國於 APEC TEL、Meridian、GFCE 等國際社群之參與，除維持會員資格及出席相關會議外，並爭取擔任召集人、督導委員或參與工作組等角色，強化我國於國際資安社群之參與深度與能見度。另視業務規劃及合作機會，推動與國際研究機構或專業社群之交流合作，包括參與台澳資安對話、相關國際研討會或投稿發表(如 CyCon)，或短期研究交流、專家互訪等，拓展我國於國際網路防禦研究社群之專業鏈結。

協助規劃並辦理每年 2 場關鍵基礎設施防護相關資安工作坊或研討會，與理念相近國家資安機構及國際資安夥伴共同進行交流，針對新興威脅趨勢、資安治理挑戰、關鍵基礎設施防護、資安演練及跨國協作等議題深入討論，促進國內外經驗交流，強化我國關鍵基礎設施資安防護能量與國際合作基礎。

- 資安服務團

依中小企業資安需求規劃培訓與顧問諮詢服務，內容依中小企業資安需求進行設計，並聘請具實務經驗之專家輔導，協助中小企業掌握資安趨勢與實務重點。規劃顧問諮詢服務，由資安輔導員協助企業診斷所提問題現況，提供企業專屬建議以利後續改善。

(3) 深化網路防禦縱深，導入主動防禦機制

- 情資研析與領域聯防
  - 國家聯防監控

    精進國家聯防監控中心(SOC)運作機制，並落實查核及驗證各機關回傳之聯防監控情資；透過全面彙整與深層分析各領域之網路攻擊與威脅情資，定期產製「資安聯防監控月報」回饋公務機關，以精準掌握整體政府資安威脅態勢與防護成效。

  - 政府領域威脅戰情分析

    深化政府骨幹網路威脅分析機制，即時掌握新興網路攻擊手法與外部資安漏洞情資；主動清查並確認政府機關受影響範疇，俾利及時發布預警，協助機關啟動應變與防禦措施。

  - 黑名單自動化阻擋

    持續維運「自動化黑名單部署服務系統」，高度整合惡意中繼站(C&C)、惡意程式下載站、釣魚郵件、弱點攻擊及帳密暴力破解等本院收容之威脅情資，提供各機關自動化讀取服務，以利即時部署於防火牆與 DNS 設備，達成主動防禦之聯防效益。

    本(116)年持續針對尚未導入服務之 A、B、C 級機關，辦理線上推廣說明會，深入解析系統架構、申請流程與實務操作，以加速驅動機關全面導入。

  - 誘捕偵測資安防護

    為掌握我國潛在之整體網路攻擊威脅，本院彙整收容各來源之外網蜜罐(Honeypot)威脅誘捕情資，並結合自建蜜罐系統蒐集之攻擊資料，藉此剖析國內外之網路威脅與攻擊樣態。

    針對外網誘捕分析，擷取並分析外網蜜罐之威脅資料，依攻擊跳板來源 IP 之行為進行分類，包含通訊埠掃描、特定服務掃描、帳號通行碼暴力破解及弱點漏洞攻擊等，據以產製入侵指

標(IoC)作為資安防護之情資應用，並定期維護收容機制以確保資料完整性。

針對已導入之資訊資源向上集中政府機關內網威脅誘捕機制，將持續維持收容內網威脅誘捕日誌回傳至本院，檢視誘捕日誌確認機關內網是否存在可疑之連線觸發事件，如發現可疑之連線觸發事件，將彙整相關資訊通知機關調查與釐清內網是否存在駭侵活動，以利機關及早預警處理。

– 惡意電郵偵測防護及研析

維運政府骨幹網路閘道(GSN)及政府機關(含重點機關與資訊資源向上集中機關)之惡意郵件偵測機制，不定期執行現場服務與設備更新，掌握政府所遭受之惡意電子郵件攻擊態勢，並按月適時產製資安情報。

研析各式惡意郵件威脅，包含郵件帳號通行碼外洩、社交工程釣魚攻擊、惡意程式垃圾郵件及 APT 郵件攻擊等，掌握最新情資與樣態。針對組織型攻擊，研蒐至少 2 個以上組織型攻擊態樣及防禦措施，以強化政府對 APT 郵件攻擊之防堵能量，同時藉由威脅樣態比對與中繼站資訊萃取，產製中繼站黑名單並進行情資分享。

此外，維持雲端惡意電郵陷阱(Mail Trap)正常運作，捕捉廣泛散布之各式惡意郵件攻擊來源，擴大社交工程惡意電郵之情蒐範圍。

- 主動檢測與技術實練

– 交通領域跨國攻防演練

協助規劃攻防演練平台功能與架構，包含規劃組功能、裁判組功能，以及用以模擬交通領域運作環境之資安演練場域，並於場域中依據實際資安事件納入不同攻擊手法，據以設計跨國網

路攻防演練情境，並於演練前規劃針對演練與場域防護設備辦理教育訓練與說明會議，以強化攻防雙方演練知能。

邀集國內、外資安團隊與國際組織共同擔任防禦方，辦理交通領域跨國網路攻防演練，針對資安事件進行攻擊軌跡查找與復原強化，以提高該領域人員面對資安事件之應變能力，並深化我國與國際間之關鍵基礎設施資安聯防。

– 國際資安演訓

依資安署指導，派員參與國際資安演練，如 Locked Shields 網路安全資安演練等，藉此與各國資安專家進行交流，並透過參與演練作業經驗，作為我國未來資安演練精進之參考，以強化我國政府機關與關鍵基礎設施防禦韌性。

– 資安技術檢測服務

配合資安稽核技術檢測作業與專案技術檢測規劃，執行政府機關 與關鍵基礎設施資安技術檢測專案。檢測終端設備、網路架構、網域 主機、資通系統及資料庫等，主動發掘潛在資安風險，並針對檢測結果提供改善建議，以協助受測單位厚植資安防護能量。

– 網路攻防演練

針對政府機關與關鍵基礎設施提供者之為民服務資通系統與主機，以模擬駭客方式進行資通系統攻擊演練，並搭配社交工程演練，藉此發掘潛藏之系統弱點以利強化防護，同時，持續維運社交工程演練系統，提供機關自行辦理機關人員資安意識測試。

– 協助檢測危害國家資通安全產品

依資安署需求及通知，協助檢測至多 30 個疑似危害國家資通安

全產品，初測後如具複查需求，可提供 1 次複測服務，並於完成全案檢測後提交技術檢測結果報告。

- 監控應變與防衛固本
  - 資通安全弱點通報機制

    持續維運資通安全弱點通報系統(VANS)，執行雲端平台與資源管理，落實資安署相關資安控制措施；配合資安署其他相關開發維運採購案之技術銜接，並協助規劃系統功能需求。

    持續推動共契廠商開發工具並辦理 CPE 轉換正確率測試，定期更新 CPE 格式轉換測試題庫，並將機關常用業務軟體納入測試範疇。

    推動共契廠商開發弱點比對工具，提供共契廠商申請弱點管理功能展示，以確認該工具是否與 VANS 系統具同等或以上效用之功能，並公告於 VANS 專區供機關採購時參考。

    協助資安署推動各項 VANS 業務，提供機關 API 介接 IP 開通及技術諮詢，並持續維護與更新 VANS 專區網站資訊，包含相關表單、FAQ 及推廣教材內容等。

  - 政府組態基準研究

    研究安全組態基準與部署技術，檢討與精進政府組態基準發展項目，以提供政府機關部署參考。製作安全組態基準實作文件與數位影片，透過清晰的內容說明與實作講解，加速機關完成導入作業，藉由一致性組態設定，提升整體政府資安底座韌性。

  - 駭侵研析與偵測防護

    全面分析資安事件處理、中繼站調研、EDR 回傳事件、資安健診及外部情資等各項來源收容之駭侵樣本，精準萃取網路攻擊

威脅特徵，並產製、部署偵測規則於政府骨幹偵測機制，同時配合多源情資關聯，分類歸納駭侵活動特徵，針對特定攻擊族群進行辨識與持續追蹤，以強化我國資通網路之防護能量。

– 端點偵測與資安防護

精進 EDR 資料回傳機制，並持續開放 EDR 事件資料回傳之連通測試，確保回傳過程、格式及內容欄位皆符合規範，並公布通過測試之產品白名單。持續蒐整並關聯分析機關回傳 EDR 事件資料，產出關鍵防護情資，並反饋納入 GSN 骨幹偵測防禦。

– 機關資安監控防護

針對重點機關包含總統府、國家安全會議、監察院、考試院、大陸委員會及中央銀行等機關執行 7×24 小時全天候資安監控作業，透過資安監控系統收容重點機關網路事件紀錄，運用關聯規則自動化偵測機制開立資安監控工單，並經由本院同仁判斷資安事件威脅類型，即時進行資安事件追蹤、通報與警訊發布。

– 資安警戒專案

於國家重要慶典、重大選舉或機關執行特定關鍵業務期間，成立資安警戒專案。提供 24 小時即時監控服務，識別潛在資安威脅並執行即時預警應變；依據駭侵事件量能進行告警，確保關鍵服務正常運作，並維持通報應處管道順暢。專案結束後，針對各機關通報事件之受駭情況與根因進行深度分析與精進。

– 資安事件通報諮詢與應處

接收並審核機關通報之資安事件，提供專業技術諮詢，協助通報機關依據法遵要求於限定時間內完成復原或損害管制，並提供損害管制建議。依據機關通報過程中所提出之技術支援需求，或因應特定單位檢測與駭客中繼站調研需求，成立應變處

理專案，提供遠端分析與現地調研之技術協助，全面鑑識各類數位跡證，查找事件根因並提出防護強化建議。

- 情資分享與學研前瞻

  – 資安情資分享

  持續維運「國家資安資訊分享與分析中心(N-ISAC)」平台，提供高效的情資交流與資料分享服務，並協助 N-ISAC 會員間深化互信與連結，促進跨領域情資交流與協同合作。持續精進資安威脅情資收容、整合、分析及分享之能量，豐富資安威脅指標之樣態，擴展資安情資之實務應用，供各領域做為資安控制措施強化之參考，以全面提升國家資通安全整體防護與應變韌性。

  – 資通安全弱點研析

  蒐集國內外之資安弱點情資，如 National Vulnerability Database、駭客論壇、新聞媒體及資安論壇等，針對重大弱點進行技術研析與影響評估，並蒐集弱點修補方式、緩解措施或檢測工具，適時發布警訊通知各界及早因應，以加速我國整體弱點修補之時效。

(4) 強化台灣電腦網路危機處理暨協調中心維運與精進

- 民間資安事件情資分享與協處

  維運多元資安對外聯繫管道(如網站介面、電子郵件等)，接收、彙整與分析民間企業分享之資安情資。接獲情資通報時，由專業人員與提供企業進行資訊確認與情資研析；若企業提出資安諮詢需求，從技術角度提供對應之應變指引與防護建議，以強化民間資安聯防生態系。

  研析企業分享之攻擊情資，若發現涉及非《資通安全法》納管對象之零日(Zero-Day)產品漏洞，主動與該產品供應商建立聯

繫，掌握漏洞影響與修補情形，強化整體資安防護效益，配合各領域中央目的事業主管機關調度，受理非公務機關重大受矚目個資外洩事件通報，協助主管機關執行行政檢查並檢視調查報告，以確認企業改善作為之有效性。持續蒐整上市櫃公司資安事件概況，藉以系統性掌握民間企業受駭樣態與潛在風險成因。

- 漏洞通報與揭露

維運資安漏洞通報平台，確保網站高可用性與穩定運作，持續參與美國 MITRE 之通用漏洞揭露(Common Vulnerabilities and Exposures, CVE)計畫，以 CVE 編號管理者(CVE Numbering Authorities, CNA)身分，受理、審核並發布針對我國產品存在資安漏洞疑慮之通報。

- 資安情資電子報

強化資安情資之傳播與宣導效益，每月主動蒐整國內外重要資安/漏洞相關新聞，並將企業所分享之去識別化資安情資，轉化改編為具宣導價值之資安專文與漏洞通報；整合官網之資安活動與宣導資訊，定期編製資安電子報推播予訂閱用戶與各界夥伴，俾利社會大眾與企業即時掌握核心資安趨勢，有效提升全民資安意識與防禦能量。

- 資安聯盟與推廣

發揮中立第三方資安信任平台功能，推動民間企業結盟與資安聯防，建立產業界互信與防禦力量。整合各方資源，協助成員將關鍵資安情資進行去識別化處理，並不定期派發與分享最新資安情資，促進聯盟內之安全交換。

執行常態化暗網情資監控，於發現異常時即時通報疑似受駭企業。規劃辦理企業藍隊資安演練，藉由模擬駭客攻擊情境，協助企業瞭解新興威脅趨勢與因應對策；以線上與實體雙軌模式舉

辦「台灣資安通報應變」年會，促進聯盟成員與民間企業之交流媒合。

- 參與國際資安組織活動

持續參與 FIRST 資訊安全緊急應變小組論壇、APCERT 亞太區電腦事故緊急應變組織年會、CERT-EU 年會等國際重要資安組織活動，並視業務需求及會議規劃，評估參與 RSA Conference 等國際大型資安會議或研討會，全年合計預計參與至少 3 場，掌握新興資安技術、威脅趨勢及事件應變實務，作為我國與國際資安社群交流合作之重要管道。

積極參與國際 CERT 相關組織及工作機制，擔任督導委員並參與相關工作組，拓展我國資安資訊分享、預警情資獲取、技術交流、資安演練及漏洞揭露等合作機會，強化國內資安防護及國際協防能量。

透過國際會議、雙邊專家交流、人員互訪及合作專案等方式，深化與各國國家級資安事件應變(CERT)組織之合作關係，並視會議安排分享我國資安治理實務、威脅趨勢、應變經驗及關鍵基礎設施防護成果，提升我國於國際資安社群之能見度與實質參與。

- 惡意檔案檢測服務

維運「惡意檔案檢測服務系統(Virus Check)」，確保系統穩定運作，引導本(116)年度著重於提升服務穩定性及檢測資料應用效益。系統持續提供檔案上傳與自動化分析服務，縮減人工操作流程並提升分析便利性，並透過蒐集各單位上傳之惡意檔案，動態掌握臺灣惡意檔案威脅之樣態趨勢。

(5) 強化委外風險管理

- 資安服務廠商評鑑機制推動

– 精進資安服務廠商評鑑機制

以「客觀評鑑」為轉型核心，全面盤點廠商之資安管理能力，並建立資安管理能量登錄機制。透過評鑑作業，實質檢視資安廠商是否建立有效之管理機制與完善之防護措施。本機制將從資安合規、人員專業、產品安全及資安聯防等四大面向評估廠商表現，期能透過客觀量化指標，精準掌握廠商能力現況，進而提升資安供應鏈之整體透明度與可靠度。

– 協助資安服務共同供應契約規範檢視及調修

因應《資通安全管理法》之實務需求，並全面匯集政府機關與產業各界之回饋意見，本計畫將針對共同供應契約內之資安服務採購規範與服務規格進行通盤檢視。

本案重點檢視範疇涵蓋六大類資安服務，包含資安監控中心(SOC)服務、資安健診、弱點掃描、滲透測試、社交工程演練及紅隊演練。計畫執行團隊將依據實務操作現況與檢視結果，提出具體之優化建議，並協助調整與修正相關政府採購契約文件，以確保契約規範能與時俱進，切合當前資安威脅防護之實需。

2. 預期效益

(1) 培訓資安前瞻人才，建構完善資安人才生態系

- 全面精進資安職能，強化機關治理量能

透過滾動修正「資安職能訓練發展藍圖」，全面納入新興資安議題與前沿技術課程，確保職能訓練精準契合最新法規與安全趨勢。藉由建構清晰之課程地圖與學習路徑，引導政府機關系統化推進資安人才培育策略，有效驅動資安人員專業升級，進而全面奠定機關之資安治理成熟度與主動防護能量。

- 構築縱深育成體系，厚植自主防衛量能

整合資安金盾獎之校園扎根、CTF 進階實戰之選手轉型，以及國際頂尖賽事之經費挹注，成功布建「校園扎根、產學對接、國際接軌」之三維縱深人才育成鏈，全方位厚植我國自主資安防護能量。其具體效益與政策價值如下：

– 落實校園防護意識，厚植技術人才梯隊

透過「金盾獎」之指標效應，引導在學學子深化資安防護意識與基礎學理；結合進階 CTF 技術培訓，引領基礎人才跨越瓶檻，每年穩定孵育具備漏洞挖掘、逆向工程等中高階實戰能量之資安防護種子。

– 精準對接產業職能，改善學用落差瓶頸

藉由新興職能需求引導，啟發學生對前沿技術之研究熱忱，將賽事能量實質轉化為就業即戰力，形塑兼具跨域解決問題能力與國際視野之拔尖菁英，有效滿足國內資安產業之核心人才缺口。

– 拓展國際賽事能見度，深化國家資安影響力

透過精準之經費補助，提供晉級決賽之頂尖選手堅實後盾，實質減輕團隊赴外參賽負擔，促進臺灣資安團隊與國際頂尖技術深度接軌，向國際展現臺灣關鍵之資安戰力。

(2) 強化政府資安治理，共創安全數位環境

- 深化零信任架構防禦

基於既有之零信任架構推動實作參考框架，擴充研訂「裝置代理/閘道模式(Device Agent/Gateway Model)」相關參考文件，協助機關依實際環境需求彈性導入，進一步強化政府網際服務網之防禦深廣度。

- 動態編修資安指引

規劃完成 3 份資安參考指引編修作業，提供政府機關最新之資安管理與技術實務規範；藉由指引內容之滾動式更新與適用性強化，協助各機關落實資安治理、法規遵循及風險管理要求。

- 驅動 IT 資安治理成熟度

  辦理 1 場 IT 資安治理成熟度評估機制線上教學課程，並精準輔導 5 家公務機關，有效提升其 IT 資安治理成熟度等級，持續強化機關內部之資安管理體制。

- 落實 OT 資安治理成熟度

  辦理 1 場 OT 資安治理成熟度評估機制線上教學課程，並精準輔導 5 家關鍵基礎設施(CI)提供者，以提升其 OT 資安治理成熟度等級，持續強化維運 CI 之公務機關與提供者之工控資安管理。

- 擘劃資安情資與聯防體系

  定期發布資安週報、季報及年報，提供全球與政府之資安威脅趨勢情資。年度預計提出至少 5 則政府資通安全威脅情勢與防護建議，以及 1 則新興資安攻擊面或防禦面技術研析；藉此協助機關即時掌握威脅趨勢，提升情資運用與風險預警能力，作為防護策略調整之決策依據，厚植政府整體資安聯防韌性。

- 前瞻國際資安法制觀測

  通盤掌握國際資安政策與法制演進，俾利我國多元面向資安政策之擘劃與調適；同時聚焦國際對 AI 與資安關聯政策、法制面之因應策略，為我國透過政策法制確保資安韌性提供實質建言。

- 深化 AI 政策法制研析與國際實質參與

  深入研析 AI 政策法制議題，並實質參與國際 AISI 網絡、重要國際組織之 AI 主題工作組或相關社群活動。期能結合我國身為 AI 硬體主力的產業優勢，貢獻對 AI 資安政策法制之思考，藉以啟

發我國更臻完善之 AI 產業(資安面)推動策略，並對 AI 相關資安議題之長期政策影響進行趨勢預判與前瞻因應。

- 國際資安合作交流
  - 透過拓展與理念相近國家及重要資安夥伴合作，建立穩定國際交流管道，深化情資分享、技術交流、資安演練及共同研究等實質合作。
  - 新增至少 1 家國外資安機構合作夥伴、促成至少 3 場國際交流會議，掌握國際資安趨勢與實務經驗，強化我國資安政策研析與防護量能。
  - 持續參與 APEC TEL、Meridian、GFCE 等國際社群，並辦理每年 2 場資安相關工作坊或研討會，提升我國國際能見度與跨國協作基礎。
- 資安服務團

  由實務專家輔導以提升員工資安意識並養成內部防護人才，降低人為失誤風險；同時由專屬輔導員協助診斷資安防護需求，提供客製化改善建議，協助中小企業將資源效益極大化以預防營運中斷。

(3) 深化網路防禦縱深，導入主動防禦機制

- 情資研析與領域聯防
  - 全面收容各機關回傳之聯防監控情資，精準分析防護項目落實程度與監控趨勢，協助機關掌握潛在資安威脅與防護現況，全面提升國家整體資安防護能見度。
  - 深度分析政府骨幹網路面臨之網路攻擊與系統漏洞，即時掌握攻擊脈絡，並發布威脅預警通報，協助政府機關及早強化漏洞防禦。

- 持續維運資訊資源向上集中機關之內網威脅誘捕機制，深度研析向上集中機關及其所屬子機關之潛在內網攻擊威脅，產製關鍵威脅情資進行聯防，厚植政府領域之內網主動防禦能量。
- 透過持續維運外網網路威脅誘捕資訊收容與分析機制，可即時掌握外網攻擊威脅趨勢與攻擊樣態，並將彙整分析之攻擊威脅情資定期提供予國內政府機關、N-ISAC 及美國 AIS 等單位進行防護，協助強化資安防護與威脅偵測能力。另產製蜜網誘捕攻擊威脅季報分享至國際資安組織，促進威脅情資交流與應用，提升我國整體資安聯防能量。
- 落實維運惡意電子郵件偵測機制，即時掌握釣魚郵件、惡意附件/連結、社交工程及 APT 郵件攻擊等威脅；結合雲端惡意電郵陷阱(Mail Trap)擴大外部樣本蒐集，研析攻擊特徵並產製中繼站黑名單提供機關聯防應用，有效阻斷針對政府機關之進階持續性威脅(APT)，降低受駭風險。

• 主動檢測與技術實練

- 完成至少 5 個交通領域攻擊情境設計，規劃演練賽制及計分方式，並配合演練期程籌備演練說明會議、導覽海報或簡報，另於期間擔任規劃組、裁判組與技術研討會講者，提升關鍵基礎設施人員之事件應變與復原技術。
- 參與至少 1 場國際資安演練活動，並將參演發現與實戰經驗轉化為技術通報，提供國內未來資安演練場域設計與防護之重要參考。
- 依據年度專案規劃與核定受測名單，落實執行政府機關與關鍵基礎設施之資安技術檢測，協助受測單位發掘架構與系統盲點，確保防禦無死角。
- 完成 1 場網路攻防演練活動並彙整相關成果，主動發掘潛藏於

機關為民服務資通系統之弱點，作為政策指導與防護強化之依據。

– 協助完成危害國家資通安全產品檢測，並產出 20 份精準之技術檢測結果報告，提供資安署作為政策研判與危害程度評估之關鍵依據。

- 監控應變與防衛固本

– 持續維運與精進資通安全弱點通報系統(VANS)，有效落實公務機關資產弱點管理，並輔導、加強共同供應契約廠商之弱點管理與 CPE 格式轉換機制。

– 針對我國資通訊環境常用系統或應用程式，主動評估其潛在重大弱點，並結合國內外分析報告完成深度研析與情資分享，協助公私部門落實弱點檢測、風險評估與補強作為。

– 完成至少 2 項政府組態基準(GCB)之發展，提供政府機關一致性之設定基準，縮減駭客利用預設漏洞攻擊之機會。

– 精準萃取惡意程式之網路行為特徵，預計每年研製並驗證 4 則偵測規則並部署於政府骨幹網路設備，即時辨識潛在威脅並發布警訊，協助受駭機關應變，大幅降低駭侵危害。

– 配合法遵要求，順暢接收機關入侵事件告警資料，高效彙整 A、B 級公務機關之端點偵測事件資料並進行樣本關聯分析，以利掌握駭客之最新攻擊手法與趨勢變化。

– 針對國家重點機關提供 7×24 小時全天候資安事件即時監控服務，與原有機關一線 SOC 服務深度互補，擴大整體威脅能見度，確保關鍵威脅即時預警、即時應變。

– 於重大慶典或特定業務期間成立資安警戒專案，建立機關與各關鍵基礎設施領域主管機關之「即時應變聯繫管道」，大幅提

升應處效率與威脅早期預警能耐。

– 在資安事件發生時，協助機關完備通報程序與損害管制；派員執行技術支援與數位跡證鑑識分析，提供具體根因改善建議，協助受駭機關重構安全防線，降低事件衝擊。

- 情資分享

精進國內資安情資分享機制，以自動化技術收整跨領域分享之資安威脅指標，提升情資之整合應用與可用性；建置國際資安威脅指標自動分享平台，對接國際 CERT 組織，深化跨國資安聯防。

(4) 強化台灣電腦網路危機處理暨協調中心維運與精進

- 透過多元管道完備情資鏈結，擴大民間企業與供應鏈之漏洞情資共享範疇，並藉由技術審查個資事件報告，系統性去識別化萃取民間受駭情資與潛在風險成因，以豐富國內民間資安情資池，促進公私協力聯防。
- 透過漏洞通報與揭露機制，促使廠商修補漏洞並提供更新，降低產品漏洞造成之危害。發布通用漏洞與暴露(CVE) 編號，協助全球資安社群進行資產盤點、溝通及識別需要更新之軟硬體。
- 每月發布 1 份資安情資電子報，將企業實戰情資成功轉化為預警與漏洞通報素材，透過主動發布與傳播，實現情資回饋民間之綜效，深化產官學研整體防護意識。
- 發揮中立第三方信任平臺之公信力，實質促進聯盟成員間去識別化情資之安全交換，搭配常態化暗網監控通報，降低企業受駭空窗期，辦理「企業藍隊資安演練」與「台灣資安通報應變年會」各 1 場，驅動情資在聯防網路內的雙向流動，全面落實以情資分享為核心之民間資安聯防機制。
- 透過參與至少 3 場國際大型資安會議或研討會，掌握國際資安政

策與技術發展趨勢，並分享我國資安治理實務、威脅趨勢及關鍵基礎設施防護經驗，深化與國際資安社群之合作關係，提升我國於全球資安議題討論及合作機制中之參與深度與能見度。

- Virus Check 服務提供我國分析可疑檔案管道，協助縮短檔案初步研判檔案惡意與否之時間，並降低惡意程式被持續誤傳擴散之風險。透過檢測資料累積與趨勢分析，精準掌握國內常見惡意檔案類型及攻擊手法，作為威脅研析、防護規則優化及資安情報產製之基礎。

(5) 強化委外風險管理

藉由推動資安廠商評鑑機制之轉型，預期將達成3項核心效益，首要，能實質強化資安服務廠商之自主資安管理能力與防護水準；其次，透過規格調修與評鑑篩選，將進一步建構安全、穩定且具備高韌性之國家級資安供應鏈體系，有效降低供應鏈受駭風險；最終，期能以此促進國內資安產業之永續發展，並協助優秀廠商接軌國際標準，形塑國際市場之競爭優勢。

3. 經費需求

本年度推動預算為 544,450 千元。

(二)關鍵基礎設施資安防護計畫

1. 業務內容

本計畫聚焦於營運科技(Operational Technology, OT)領域之資安強化，首先透過各關鍵領域之多方面工控資安檢測，了解與輔導現行架構之威脅；其次以 OT 數位靶場引導技術防護人員應變處理技能；最後以資通安全桌上推演提示高階決策人員對突發事件之即時反應。藉由系統性方式提升關鍵基礎設施之資安應變技能，並建構關鍵基礎設施提供者專屬治理架構。並於政府施政方向與監督下，逐步強化我國在 OT 資安領域之自主防禦能力，強化國家關鍵基礎設

施之數位防線。

(1) 評估、威脅狩獵、事件處理及自動化研析

聚焦於關鍵基礎設施 IT/OT 邊界與 OT 場域之資通安全評估與實務防護作業，透過實地檢測、威脅狩獵及異常行為分析，強化對潛在攻擊行為之早期辨識能力；同時結合事件處理與調查取證機制，提升資安事件發生時之應變效率與處置品質。在技術發展面，持續推動 AI 導向自動化研析工具之優化與驗證，逐步導入至實際場域，協助檢測人員進行威脅研判與分析作業，降低人工作業負擔，並提升整體防護作業之一致性與可複製性。

(2) 數位靶場與資通安全桌上推演

強化人員實戰能力與組織韌性為主要目標，延續並強化模擬真實工控系統架構與攻擊情境之數位靶場環境，提供擬真攻防演練場域，培育具備實務經驗之技術防護人才；同時透過資通安全桌上推演，模擬重大資安事件發生時之決策流程、跨單位協調與資源調度情境，強化高階管理與決策層之應變能力，並在符合相關規範之前提下，促進跨領域協作與溝通能力提升。

2. 預期效益

(1) 評估、威脅狩獵、事件處理及自動化研析

透過人力擴充、技術深化、檢測量能提升及自動化應用並進之策略，建構由評估、偵測、應變至精進之完整防護循環。此舉將實質協助我國關鍵基礎設施由過往之「合規導向」資安管理模式，逐步轉型為以「實戰與韌性」為核心之動態防護體系，為後續年度之持續擴展與長期營運奠定穩固基礎。

(2) 數位靶場與資通安全桌上推演

成功建構國內專屬之工控系統數位靶場，有效厚植關鍵基礎設

施防衛方(Blue Team)之實戰防禦技能；同時，透過高風險情境之桌上推演，可強化高階資安應變決策人才之布局，促進跨部門及公私協作之默契，從技術層與策略層雙管齊下，打造具備高度彈性與耐受力的組織韌性體系。

3. 經費需求

本年度推動預算為 313,200 千元。

(三)AI 網路威脅偵防技術研究計畫

在全球數位轉型趨勢下，資安威脅日益複雜。為改善傳統資安防護依賴人工規則與專家判斷所造成的效率與人力負擔，本計畫導入 AI 技術，聚焦多源情資整合視覺化與 AI 攻擊預測結構化知識萃取，規劃「可視化即時情資平臺」及「跨域 AI 攻擊預測模型」兩大工作項目與執行內容，以達成計畫目標與效益。

1. 業務內容

(1) 前瞻資安技術發展：可視化即時情資平臺

本技術旨在因應資安署推動資安網路防禦技術 AI 化政策方向，透過 AI 驅動之多維資料整合與視覺化技術，串接 N-SOC、N-ISAC、N-CERT、GSN 等多元異質情資，並以標準化 API 接口收容各來源資料，透過通用資料模型(Common Data Model, CDM)進行欄位對齊、格式轉換與去識別化，建立具跨來源關聯分析能力之結構化情資資料庫；同時以事件驅動之 AI Agent 框架為核心，當情資資料庫接收新事件時自動觸發分析 Agent，執行多維關聯分析、威脅評級與告警推送，並將結果彙整呈現於視覺化戰情儀表板，協助管理者快速掌握整體安全態勢、即時威脅趨勢，並提升主動式防禦能力。

(2) 推動資安網路防禦技術 AI 化：跨域 AI 攻擊預測模型

本技術作為可視化即時情資平臺之後端 AI 推理引擎，負責從 N-

SOC、N-ISAC、N-CERT、GSN 等多源原始情資中，運用地端部署之大型語言模型(LLM)自動萃取結構化威脅知識並預測攻擊途徑。116 年度聚焦完成 IoC(入侵指標)及威脅情境二類結構化知識之萃取與自動化輸出，TTPs、趨勢預測及防禦策略三類將於 117 年以後依技術成熟度依序擴展；並提供自然語言查詢介面及 IoC 可信度評分模型，供資安人員快速掌握威脅態勢與篩選高可信度情資。本工項研發均採 FDE(Forward Deployment Engineering)精神執行，開發前先確認業務單位實際需求，並以資安院為驗證場域迭代優化模型與介面設計。

本工項延續 114-115 年度已建立之語意化系統、知識庫及模型調度層架構，並依委員意見落實 FDE 精神，於開發前確認業務單位實際需求，以資安院為驗證場域迭代優化模型與介面設計，確保研發成果符合實務需求

2. 預期效益

(1) 前瞻資安技術發展：可視化即時情資平臺

- 情資來源整合數：116 年度完成 1 個來源(GSN)之單一戰情呈現。
- 場域覆蓋數：116 年度完成 1 個場域(資安院)之戰情儀表板實地部署。
- 儀表板更新頻率：每 10 分鐘內自動更新一次戰情資訊。
- 視覺化呈現維度：涵蓋攻擊來源分布、受影響機關統計、威脅趨勢時間軸等 3 類核心視覺化元件。

(2) 推動資安網路防禦技術 AI 化：跨域 AI 攻擊預測模型

- 建立 LLM 威脅情資推論能力

情資自動化分析時間縮短 50%以上，人工平均處理時間由現況降至 60 分鐘以內；116 年完成 IoC 及威脅情境二類結構化知識

輸出，準確率達 85%以上(TTPs、趨勢預測及防禦策略於 117 年以後逐年擴展)。

- 完成跨域場域實證與技術擴散

116 年度優先以 GSN 情資進行模型分析與驗證，並以標準 API 供至少 1 個政府機關或關鍵基礎設施(CI)介接運用，介接成功率達 100%；於資安院完成 1 個場域單位之試行驗證。

3. 經費需求

本年度推動預算為 93,786 千元。

(四)數位訊息分析技術研發計畫

1. 業務內容

研發數位訊息分析技術，強化數位訊息威脅情資共享與分析能力，建立政府與民間單位數位訊息威脅應對體系，強化國家總體韌性與國家安全，深耕民主並推動台灣成為全球公民科技發展場域。

本計畫採取階段性策略推進，於 114 年完成概念驗證、115 年實現落地應用後，於 116 至 118 年將進一步完成「專用模組開發」、「國際推廣」，並持續針對服務進行迭代更新，最終目標是建構兼具效率與韌性的防禦體系，確保我國在資訊戰與認知戰的挑戰下，仍能維持民主制度穩定與社會信任基礎。

(1) 強化數位訊息威脅情資共享與分析能力

以 115 年度「數位訊息威脅情資共享平台」所累積之情資總數為基準，藉由 116 年導入公共情資共享機制，擴充高風險數位訊息威脅情資數量 20%以上，並產出系統資料庫增長數據佐證報告；提升數位訊息情資共享資料品質，以 115 年度該平台所建立之不同情資來源關聯分析總數為基準，增加 20%以上成功關聯分析件數，強化數位訊息情資分析能力。

(2) 建立政府與民間單位數位訊息威脅應對體系

規劃累計完成至少 3 間具指標性公私部門機構之專用模組深度導入與場域驗證(PoC)，於導入後，將透過嚴謹之問卷調查進行成效追蹤，目標使機構端針對「威脅情資識別」、「多來源訊息分析」、「人工智慧威脅內容鑑識」等專用模組之適用性滿意度評價，平均達 3 分(滿分 5 分)以上。此外，在實務作業效能層面，專用模組導入後，將經由內部或第三方效能評估結果驗證，確保受測機構產出數位訊息威脅分析相關報告之平均耗時，較導入前縮減(或產出效率提升)達 20%以上，達成作業流程精簡與即時應變之目標。

2. 預期效益

(1) 技術與情資面：強化公私部門數位訊息威脅應對效能

- 情資規模化與多樣化

針對核心指標性公私部門機構，深度導入「威脅情資識別」、「多來源訊息分析」及「AI 威脅鑑識」等專用模組，預期達成 3 間以上機構之落地驗證，並確保機構端之模組適用性滿意度達 3 分(滿分 5 分)以上，實質將研發技術轉化為第一線之防護力。

- 分析工具 AI 化

結合 AI 自動化工具與深度學習模型，取代傳統人力分析流程，預期提升 20% 以上的跨來源情資關聯分析成功件數。透過自然語言處理(NLP)與多模態分析，強化對生成式 AI 濫用及跨語言(中、英、西文)訊息的識別精準度。

(2) 實務應用面：建構高韌性數位訊息威脅聯防體系

- 場域驗證與模組落地

針對指標性公私部門機構導入「威脅情資識別」、「多來源

訊息分析」及「AI 威脅鑑識」等專用模組，預期達成 3 間以上機構之深度導入。目標使機構端對模組適用性之滿意度達 3 分(滿分 5 分)以上，確保技術轉化為實際防護力。

- 作業效率大幅提升

  透過自動化與 AI 技術導入，預期使受測機構產出數位訊息威脅分析報告之平均耗時縮減(或效率提升)20% 以上。這將使第一線應對單位能以更短的反應時間對抗瞬息萬變的數位威脅。

- 國家安全與戰略面：建構跨國界與跨領域之防衛體系

  – 維護國家安全與社會穩定

  緊密整合國安、警調、政府及學術單位需求，發展針對全球華文社群的開源情資分析工具。藉由追蹤人工智慧威脅內容的散播路徑，能提前預知異常特徵，有效反制境外或惡意之資訊操弄干預。

  – 提升國際影響力與外交合作

  建立跨語言訊息分析框架與情資共享機制，除能滿足外交單位對國際情勢的掌握外，更可藉由技術輸出與情資交換，強化台灣在國際數位防衛領域的指標地位，建構跨國界的情資聯防陣線。

3. 經費需求

本年度推動預算為 90,160 千元。

(五)全民資安意識與韌性延伸推動計畫

1. 業務內容

本計畫旨在增進全社會的資安防護意識，觀察我國現況，雖已累積強大科技實力與成熟的專業資安資源，但在全民推廣上仍面臨資源散落各部會、內容過於生硬及族群識能落差等挑戰。為此，本

計畫導入分眾轉譯與賦能實作等策略，以開發與整合資安意識資源，並發展校園、非營利組織與社區之資安共學模式，預期將艱澀技術轉化為直覺的生活知能，將資安意識由單點宣導延伸至全民日常生活，具體落實《第七期國家資通安全發展方案》中「推動社會資安意識提升」之政策指標。

(1) 全民資安意識推廣研究與推動策略研析

聚焦於建立我國全民資安意識推廣之決策基礎，作為後續推廣行動的策略方向。除蒐整國內外資安意識與行為改變之相關研究外，亦將回顧與盤點我國過去各部會執行資安意識推廣措施之成果與限制，檢視既有推廣模式之成效與不足，作為後續策略調整與資源配置之依據。透過結合行為科學、認知心理之視角，針對不同族群在不同資安情境下的風險感知及行為落差進行研析，完成年度推廣研究及建議報告，以確保整體計畫推廣走向，並以實證研究驅動、策略一致的全民資安推廣藍圖。

(2) 資安意識資源標準規範建構與整合導引機制

現行資安推廣資源多以行政分工或專業視角呈現，對於未具備資安背景之民眾、組織與中小企業而言，往往難以判斷「這個資源是否適合我、在什麼情況下該使用」，造成近用困難與實際效益有限。為解決我國全民資安推廣長期面臨的「資源碎片化與近用困難」問題，本計畫將以「資安意識資源圖鑑」為核心，建構以使用者身分與情境為導向的國家級資安資源索引與導引體系。透過盤點並整合分散於各部會、學研機構與民間社群之資安推廣資源，完成資安資源規格化管理架構與標籤分類規範，透過使用者需求的設計原則，並完成「全民資安共學共創平台」網站架構設計，使不同來源、不同形式的資源得以被放入同一套架構中，並可持續更新與重複利用。

(3) 多元分眾資安教材教具研發

以「將認知轉化為行為」為核心目標，依據前述研究成果，發展適合不同族群使用的資安教材與教具，並透過社會共創機制，擴大資安教育的創新與擴散效應。本計畫將跳脫傳統說明式教材框架，強調以情境導向、互動參與及低門檻設計，引導民眾在日常情境中建立正確資安行為。

(4) 跨域韌性延伸推廣活動落實在地化

本計畫著重於將前述主軸策略研析成果、教材資源導入實際生活場域，依據建構之分眾樣態設計對應形式，透過在地共學、校園試行與大型體驗活動，促使資安意識成為日常行為的一部分，建立多次接觸、反覆練習與社會互動的推廣機制，促使資安意識逐步內化為可持續的日常習慣與群體共識，強化全民主動防禦基礎。

2. 預期效益

(1) 全民資安意識推廣研究與推動策略研析

透過年度推廣策略研究與國際趨勢分析，建立符合我國社會環境之全民資安推廣架構，作為後續教材開發、資源整合及推廣活動規劃依據。預期可提升宣導資源配置精準度，強化各族群資安需求辨識能力，並建立可持續追蹤與滾動調整之推廣機制，提高資安意識政策推動效益及社會韌性建構成效。

(2) 資安意識資源標準規範建構與整合導引機制

成功建立全國首套資安資源分類與標籤規範，促進政府、民間及教育單位資安資源之系統化盤整與橫向共享，有效降低資源重複開發之行政與搜尋成本。

奠定未來「全民資安共學共創平台」之基礎底座架構，大幅提升資安資源之可近性與再利用率，逐步形成跨機關、跨領域之動態

資安知識共享網絡。

(3) 多元分眾資安教材教具研發

透過開發至少 8 套分眾教材教具，協助不同族群將資安知識轉化為具體防護行動。預期可提升民眾對常見資安風險之辨識能力與防護意識，並透過部分教材中之自我檢核機制，引導使用者檢視個人防護行為，達成超過 70%使用者完成基礎防護行為檢視與實踐，降低因資安認知不足所造成之數位風險，逐步縮減不同族群間之數位落差。

(4) 跨域韌性延伸推廣活動落實在地化

透過徵件活動導入資源圖鑑、數位策展及在地共學機制，透過校園場域試教試玩完成教學模組測試與回饋、資安共學形式完成非營利或社區型組織資安識能共學，擴大資安議題觸及範圍，預期累積線上及實體資安知能觸及與曝光達 25 萬人次以上，並成功促成非營利組織(NGO)及社區團體深度參與資安推廣行列。

藉由行為檢核與實際應用驗證，預期促使 60%以上之活動參與者產生具體之資安防護行動意向，或實質完成關鍵防護措施之設定，全面提升社區層級之數位韌性與自主防護能力。

3. 經費需求

本年度推動預算為 20,400 千元。

(六)提升通傳領域資安聯防機制及強化通傳網路預警應變能力

1. 業務內容

提升通傳網路資安監控、分析通報與應處能量，持續強化 SOC、ISAC、CERT 及 C-NOC 等核心業務運作，並辦理攻防演練、教育訓練、交流會議及資安稽核；同時導入雲端架構機制，提升網路障礙通報等服務穩定性與營運韌性。

相較前一年度，本年度除持續辦理通傳領域資安監控、通報、演練、訓練及稽核等例行工作外，將進一步強化海纜情資自動化分享、多維度圖層展示及 EMIC 等資料交換介接機制，提升海纜障礙情資傳遞效率；並透過 NCCSC 情資自動化處置能力優化，縮短資安事件分析與通報作業流程，提升通傳領域資安聯防之即時性及可操作性。

(1) 優化國家通訊暨網際安全中心(NCCSC)之威脅預警與情資自動化處置能力

著重於深化 NCCSC 之全天候(7×24 小時)即時監控與自動化通報機制，俾利即時精準掌握海纜障礙等重大國土安全事件與突發資安事件。系統於偵測威脅時，將自動分別向「國土安全事件通報系統」及國家資安應變中心(N-CERT)辦理即時通報，並持續進行多源資安情資之彙整、分析與情資分享。此外，將積極配合主管機關，落實資安責任等級 A 級機關之各項法定應辦事項，全面強化通傳領域之資安預警、跨域聯防及事件應變效能。

(2) 完善障礙通報機制，強化海纜通報效率

持續精進 C-NOC 系統障礙通報及海纜情資展示功能，全面提升通信網路與海纜障礙資訊之蒐整、通報及分享效率。本年度將重點建置海纜情資與災害防救資訊系統(EMIC) 之資料交換介接模組，促進跨部會情資交換與即時掌握海纜障礙狀況。透過自動化通報及多維度圖層展示，縮短業者填報及機關掌握資訊所需時間，確保通傳網路順暢運作。

(3) 提供通傳 CI 提供者資安事件技術支援及協處

建立完善之緊急資安事件應處支援機制，針對通傳領域 CI 提供者發生之資安事件，由專業技術團隊即時提供包含技術研判、事件鑑識分析及處置應變建議等一站式服務。協助受駭單位釐清資安事

件樣態、駭客入侵路徑、潛在影響範圍與實質損害情形，並提出針對性之根因改善及系統復原建議，協助 CI 提供者於最短時間內完成損害控制，將資安事件之衝擊降至最低。

(4) 辦理通傳事業資安攻防演練、教育訓練及情資分享會議

為精進整體通傳事業資安防護能量與應對能力，辦理通傳事業資安攻防演練、資安教育訓練及情資分享會議，強化通傳事業資安防護及應變能力。每年辦理資安攻防演練 1 場次、資安教育訓練 4 場次，並辦理通傳領域資安聯防相關會議 4 場次。透過實兵演練、技術培訓與跨業情資交流，全面提升關鍵基礎設施與特定關鍵基礎設施從業人員之資安防護意識，使其熟稔資安事件之緊急應變標準作業程序。

(5) 辦理通傳領域關鍵基礎設施提供者資安稽核作業

依資通安全管理法規定，辦理通傳領域關鍵基礎設施提供者資通安全維護計畫實施情形稽核作業。每年辦理 6 家通傳領域關鍵基礎設施提供者稽核，檢視其資安維護計畫落實情形及防護作為。透過稽核發掘缺失並提出改善建議，協助受稽單位持續精進資安管理與防護水準。

(6) 辦理公眾電信網路資通安全檢驗稽核作業

依電信管理法等法規規範，辦理公眾電信網路資通安全檢驗稽核作業，檢視業者資通安全設備、管理制度及防護措施落實情形，規劃每年辦理 3 家公眾電信網路資通安全檢驗稽核，督導業者符合相關法規及資安要求。透過定期或不定期檢驗，確保公眾電信網路維持安全、穩定及可信賴之運作。

2. 預期效益

- 預計完成 NCCSC 全天候威脅預警與情資處置機制之深度優化，全面強化對於通傳領域關鍵基礎設施網路運作狀態與障礙資訊之

主動掌握能力。

- 順利完成 C-NOC 系統通報介接功能優化，以及海纜情資自動化分享機制之建置，實質提升海纜障礙通報效率與跨單位情資交換之格式一致性。
- 本年度預期辦理通傳事業資安攻防演練 1 場次、專業資安教育訓練達 4 場次、資安聯防相關會議 4 場次；並完成通傳領域關鍵基礎設施提供者資安稽核 6 家，以及 3 家公眾電信網路業者之資通安全檢驗稽核，有效協助整體通傳產業界強化法規遵循、事件緊急應變與自主資安防護能力。
- 逐步推動 NCCSC 雲端化服務平臺建置，本年度完成 C-NOC 系統平臺第一階段之上雲部署與架構驗證提升核心系統服務韌性、資安防護及持續營運能力。

3. 經費需求

本年度推動預算為 93,413 千元。

(七)資料保護驗測機制推動計畫

1. 業務內容

本計畫將以提升我國資料保護與風險評估能力、降低機關及產業導入門檻、促進可信任資料共享與創新應用為目標。透過建立兼顧隱私保護與資料利用之技術、驗測及治理機制，推動隱私強化技術與合成資料於實際場域落地應用，進一步強化資料治理量能，支撐數位治理與 AI 創新發展。

緊密銜接既有之隱私強化技術應用指引、資料保護驗測機制及「PETsARD」等階段性推動成果，規劃於 116 年度持續深化資料保護之技術研究、制度精進及推廣應用，加速將既有研究成果轉化為實務應用能力。

本工作項規劃由「制度面」、「技術面」、「工具面」與「推廣面」等四大構面同步推進，具體執行內容如下：

(1) 制度面研析與規範銜接

持續且系統化地研析國際資料保護政策、法規(如歐盟 GDPR 等)及最新技術發展趨勢，藉以動態強化我國隱私強化技術應用指引，並精準調修國家標準規(CNS)與驗測機制間之銜接與參照關係，建構與國際接軌之合規治理架構。

(2) 技術面深化與風險控制

聚焦於合成資料生成、隱私風險控制及人工智慧資料利用等關鍵核心議題。研發團隊將積極發展兼顧隱私保護與資料效用規(Data Utility)之優化技術方法，並針對多元產業與政府實際應用情境進行可行性評估與壓力測試，確保技術方案之安全與實用性。

(3) 工具面優化與實務驗測

配合前述最新技術研究成果，持續優化現行資料保護評估工具與自動化驗測機制。本年度將重點提升系統對於非結構化資料、多源異質資料等多元資料型態之支援能力，實質強化檢測工具之實務可用性與作業效率。

(4) 推廣面培力與跨域交流

規劃透過辦理大型技術競賽、專業培訓課程、實作工作坊、國際學術與產業交流會議，以及全民 PETs 意識推廣活動，橫向擴大隱私強化技術之社會知曉度與產業應用率，由下而上逐步建立兼顧資料安全與價值挖掘之發展環境。

2. 預期效益

(1) 強化多元資料處理能力並控制隱私風險

透過制度研析、技術研發、工具優化及推廣培力等工作之全面

落實，預期將實質強化我國運用隱私強化技術處理多元資料之核心能力，有效降低資料流通與人工智慧發展過程中的隱私洩漏風險，大幅降低公私部門之技術引進門檻。

(2) 累積實證成果以優化國家資料治理政策

藉由實際場域之落地應用，本計畫將成功累積資料保護與資料利用平衡之實證數據與示範案例，作為未來國家級資料治理、可信任 AI 政策規劃與法制修訂之前瞻科學參據。

(3) 提升社會認知並奠定可信任利用基礎

藉由多元競賽、專業課程、實務工作坊及全民宣導活動之辦理，預期將顯著提升政府、產業、學研界及社會大眾對於隱私強化技術之認知度與信賴接受度，逐步建構我國邁向數位智慧社會所需之可信任資料利用體系。

3. 經費需求

本年度推動預算為 25,620 千元。

(八) 中小企業及產品資安強化計畫

1. 業務內容

本計畫旨在透過強化產品資安韌性、供應鏈資安治理及產品漏洞管理，推動漏洞通報與漏洞獵捕(Bug Bounty)機制、建置產品資安測試場域及深化專業人才培育，積極促進產、官、學、研與白帽駭客社群之跨域協作，據以建構完善之產品資安與供應鏈安全防護生態系，實質提升我國資通訊產品及服務之資安韌性與國際市場競爭力。

(1) 強化產品資安韌性

- 資訊服務業者聯合稽核

將協助資通安全署針對國內重要資訊服務業者辦理資通安全

聯合稽核作業，每年擇選至少 10 家重要資服業者實施聯合稽核，以強化政府資訊服務供應鏈之資通安全管理。工作內容包含規劃稽核時程、籌組稽核小組、辦理稽核前溝通協調及執行資通安全聯合稽核作業，並彙整稽核結果與共同發現事項，提出改善建議供相關機關及業者參考。

- 建置國家級漏洞獵捕(Bug Bounty)計畫場域

規劃由政府建立中立之漏洞獵捕活動運作機制與測試場域，整合政府、產業、資安研究人員及白帽駭客社群能量，建立可長期運作之漏洞通報、驗證、修補及追蹤流程，形成安全研究、漏洞通報與產品改善之合作模式，提升我國資通訊產品及服務安全性。

持續建置國家級漏洞獵捕場域，規劃活動運作制度，包含標的遴選、研究人員參與、漏洞受理、風險分級、修補追蹤及成果回饋等流程，並挑選高風險或廣泛應用於政府機關之軟硬體產品與服務作為年度測試標的，辦理漏洞獵捕活動，產出專業可信賴之漏洞風險驗證成果。

因應歐盟《網路韌性法》(CRA)及國際產品資安治理之最新趨勢，本計畫將持續且系統化地研析國際間關於產品資安法規、漏洞管理、軟體清單(SBOM)及開源社群等前瞻議題，作為我國推動產品資安治理之政策藍圖參考。同時，本工作將結合共同供應契約廠商之輔導機制，實質協助合約業者導入產品安全事件應變團隊(PSIRT)之標準化作法，全面完善漏洞接收、評估、修補、揭露及對外溝通流程，逐步建立常態化漏洞獵捕生態系，厚植政府採購供應鏈之數位韌性。

(2) 提升中小企業資安防護

以強化基層資安人才根基與提升產業基礎資安韌性為雙軌目

標，引入美國網路安全診所聯盟(Consortium of Cybersecurity Clinics, CCC)之課程概念，本計畫規劃與國內大專院校合作開設「網路安全實務與社會」實踐課程，積極培育有志運用資安專業知識、從事社會服務之校園優秀人才，使其成為具備實務能量之「學生輔導員」。由教學團隊與學生輔導員共同組成「資安健檢團」，協助我國中小企業進行漏洞掃描與防護合規檢視，協助中小企業增進資安風險意識並提升第一線之資安實務防護能力。

2. 預期效益

(1) 降低重複稽核行政成本與提升委外品質

透過推動資服業者聯合稽核，能有效減少各政府機關單獨辦理委外廠商稽核時所耗費之行政成本，同時解決資服業者因面臨不同機關頻繁稽核，導致作業時間冗長與人力資源重複投入之結構性問題，進而顯著提升政府機關委外品質與產業整體之服務效能。

(2) 建構常態化漏洞治理與健全防禦韌性

成功建立常態化之漏洞通報、驗證與處理機制，實質協助資通訊產品製造商與資服業者完善其產品安全事件應變團隊(PSIRT)及漏洞生命週期管理流程。藉由深度掌握國際產品資安法規及治理趨勢分享，提供我國政策訂定之參考，從源頭降低政府資訊服務供應鏈之資安風險，全面強化我國資通訊產品與服務之安全性。

(3) 深耕產業支援網絡

透過與大專院校之產學合作，預期每年協助至少 20 家中小企業完成之資安健檢服務，並產出客製化之改善建議報告，縮短中小企業導入資安防護之摸索期，減輕其成本負擔。

(4) 量化指標追蹤與抗壓提升

工作將透過「改善建議完成率」與「服務滿意度(目標達 80%以

上)」等關鍵量化指標，嚴謹檢視與滾動修正，逐步建構具備永續運作動能之產業資安支援網絡，全面提升我國中小企業面對新興資安威脅之應變效率與整體產業之風險承受能力。

3. 經費需求

本年度推動預算為 35,000 千元。

(九)年度目標

本院 116 年度各補助計畫工作項目年度目標，詳見表 3。

表3　補助計畫工作項目年度目標

計畫名稱	工作項目	年度目標
116 年政府資通安全防護工作執行計畫	推動現行資安職能基準及培訓	發展資安人才生態系，厚植基層防護能量
	辦理資安技能競賽金盾獎	扎根校園資安，精進在學學子實戰技術與防護意識
	活絡國內資安賽事生態	深化進階資安攻防技術培訓，培育符合新興職能需求之跨域中高階資安人才
	凝聚國際資安賽事團隊	挹注頂尖戰隊赴外參賽能量，深化臺灣資安技術之國際能見度與影響力
	零信任架構資安防護	建構政府機關與防禦場域之資安信任治理環境
	編修資安參考指引	定期檢視資安規範發展藍圖，依藍圖時程編修實務指引
	推動 IT 資安治理成熟度	精進公務機關之資安治理架構，強化內部合規度
	推動工控領域(OT)資安治理成熟度	持續精進 OT 資安治理成熟度機制與評估問項，並協助推動 OT 資安治理成熟度評估作業
	資安刊物編審與發布	定期蒐集國內外資安威脅情資、重大資安事件、漏洞資訊及政策動態
	國際資安政策法制觀測與研析	定期執行國際資安法制觀測，維持政策前瞻性
	AI 政策法制議題研析與國際活動之參與	1. 挑選並研析最新且重要之 AI 政策法制議題

計畫名稱	工作項目	年度目標
		2. 參與會議、研討會或其他交流機制，參與國際 AISI 網絡、其他國際組織之 AI 主題工作組，或其他國際機構、相關社群之討論或活動
	國際資安合作交流	1.持續拓展我國與理念相近國家、國際資安組織、國家級資安機構及重要技術/研究單位之合作 2.深化我國國際資安合作網絡，強化跨國資安聯防、關鍵基礎設施防護及國際資安社群參與能量
	資安服務團	規劃顧問諮詢服務，由資安輔導員協助企業診斷所提問題現況，提供企業專屬建議以利後續改善
	國家聯防監控	持續收容公務機關與特定非公務機關之監控情資，精進聯防監控資料之回傳與監理機制
	政府領域威脅戰情分析	持續分析政府機關網路威脅與漏洞情資，確認影響範圍
	黑名單自動化阻擋	推動公務機關及特定非公務機關導入黑名單自動化部署服務
	誘捕偵測資安防護	維持外網與內網威脅誘捕資訊收容機制之穩定運作
	惡意電郵偵測防護及研析	維持政府領域惡意郵件偵測防機制穩定運作
	交通領域跨國攻防演練	完成交通領域業者需求蒐整，建置雲端化演練平台
	國際資安演訓	參與國際網路安全資安演練，精進國內情境設計
	資通安全弱點通報機制	維運資通安全弱點通報系統

計畫名稱	工作項目	年度目標
		(VANS)，並進行雲端化
	協助檢測危害國家資通安全產品	提供高風險產品之資安危害程度技術檢測
	資通安全弱點研析	持續蒐集國內外重大資安弱點，評估潛在影響
	政府組態基準研究	檢討與精進政府組態基準(GCB)發展項目
	資安技術檢測服務	執行政府機關或關鍵基礎設施之技術檢測專案
	網路攻防演練	針對為民服務資通系統與主機進行模擬駭客攻擊演練
	駭侵研析與偵測防護	蒐集分析組織型駭侵樣本，萃取網路威脅特徵
	端點偵測與防護	蒐整並分析機關端點防護情資，強化整體防線
	機關資安監控防護	針對重點機關提供 7×24 資安監控作業
	資安警戒專案	協助於國家重要慶典及機關執行特定業務期間成立資安警戒專案
	資安事件通報諮詢與應處	接收並審核機關通報之資安事件，同時依據需求技術協助
	資安情資分享	維持 N-ISAC 平台服務穩定運作，收整與應用外部威脅情資
	民間資安事件通報與協處	增進民間與企業資安事件情資交流與應變協處機制
	漏洞通報與揭露	維運資安漏洞通報平台，確保網站以穩定與可用之通報網站
	資安情資電子報	促進民間資安知識傳遞與威脅資訊普及

計畫名稱	工作項目	年度目標
	資安聯盟與推廣	增進企業資安實務交流並提升事件應變能力
	參與國際資安組織活動	持續參與 FIRST、APCERT、CERT-EU 等國際重要資安組織活動，掌握國際資安技術、威脅趨勢及事件應變實務，深化我國與國際 CERT 組織及資安社群之交流合作
	惡意檔案檢測服務	維持 Virus Check 惡意檔案檢測服務穩定運作
	資安服務廠商評鑑機制推動	辦理資安服務共同供應契約採購規範檢視及資安服務廠商評鑑作業
關鍵基礎設施資安防護計畫	評估、威脅狩獵、事件處理及自動化研析	檢測能量進入擴張期，推動跨產業導入，逐步建立不同領域關鍵基礎設施檢測模式
		AI 模型進入實用化階段，選定至少 1 間具代表性之關鍵基礎設施單位進行導入部署，進行效能監測與回饋優化
	數位靶場與資通安全桌上推演	完善數位靶場功能與資通安全桌上推演流程，提升模擬攻防之真實度
AI 網路威脅偵防技術研究計畫	前瞻資安技術發展：可視化即時情資平臺	本年度將整合 N-SOC、N-ISAC、N-CERT、GSN 等多源情資，透過通用資料模型(CDM)進行格式對齊與正規化，並以事件驅動之 AI Agent 架構執行多維關聯分析與威脅評級，建置具備視覺化戰情儀表板之即時情資平臺，將分散、異質之資安資訊轉化為可操作之決策依據，強化整體主動防禦能量
	推動資安網路防禦技術 AI	本年度將以地端部署之大型語言模

計畫名稱	工作項目	年度目標
	化：跨域AI攻擊預測模型	型(LLM)為核心推理引擎，收容 N-SOC、N-ISAC、N-CERT、GSN 等多源威脅情資並進行清洗與正規化，聚焦完成 IoC 及威脅情境二類結構化知識之萃取與自動化輸出，並提供自然語言查詢介面及 IoC 可信度評分模型，研發並依 FDE 精神以資安院為驗證場域迭代優化
數位訊息分析技術研發計畫	強化數位訊息威脅情資共享與分析能力	以 115 年度平台數據為基準，藉由導入公共情資共享機制，擴充高風險數位訊息威脅情資數量並強化分析品質
	建立政府與民間單位數位訊息威脅應對體系	針對指標性公私部門機構導入專用模組，以自動化與 AI 技術大幅精簡第一線單位之應變耗時
全民資安意識與韌性延伸推動計畫	全民資安意識推廣研究與推動策略研析	執行推廣策略研析，確立本土化賦能方針，納入全球資安意識趨勢，產出科學化決策依據
	資安意識資源標準規範建構與整合導引機制	研發資安資源規格化標準，整合跨域推廣資源治理，制定資安資源圖鑑分類架構與標準化標籤規範，解決現況資源分散痛點。
	多元分眾資安教材教具研發	研發情境導向與低門檻之分眾教材教具，將專業技術語境轉譯為生活可應用之資安知能
	跨域韌性延伸推廣活動落實在地化	實施在地場域共學與數位策展，串連校園試教與非營利或社區型組織，引導資安意識內化為日常習慣
提升通傳領域資安聯防機制	優化國家通訊暨網際安全中心(NCCSC)之威脅預警與情資自動化處置能力.	1. 強化通傳領域資安預警、聯防及事件應變效能

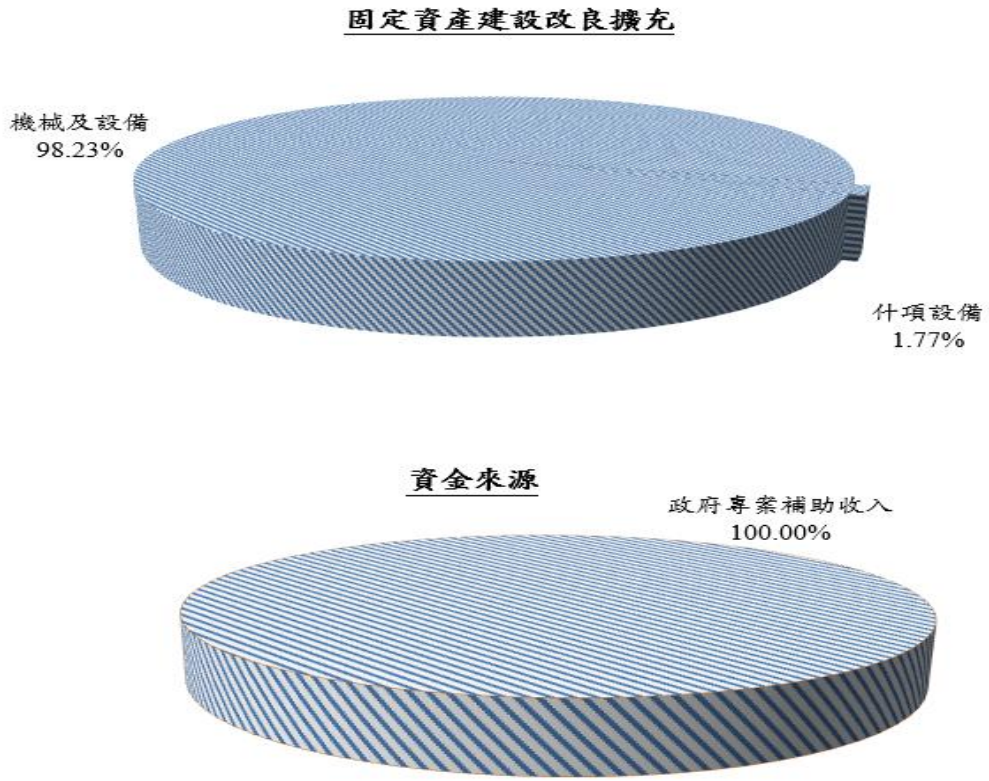
計畫名稱	工作項目	年度目標
及強化通傳網路預警應變能力	完善障礙通報機制，強化海纜通報效率	1. 推動跨機關情資交換與自動化通報
	提供通傳 CI 提供者資安事件技術支援及協處	建立通傳領域 CI 提供者資安事件技術協處機制
	辦理通傳事業資安攻防演練、教育訓練及情資分享會議	強化通傳事業資安防護、聯防協作及事件應變能力
	辦理通傳領域關鍵基礎設施提供者資安稽核作業	辦理通傳領域 CI 提供者資安稽核作業，強化關鍵基礎設施資安防護與法遵能力
	辦理公眾電信網路設置者資安檢驗作業	辦理公眾電信網路設置者資通安全檢驗，督導業者落實資安防護措施及法規要求
資料保護驗測機制推動計畫	1.制度研析與指引精進 2.關鍵技術與資料研發 3.工具優化與驗測推動 宣導推廣與人才培力	發展兼顧隱私保護與資料效用之技術方法，優化評估工具，提升各界對隱私強化技術(PETs)之接受度
中小企業及產品資安強化計畫	強化產品資安韌性	資訊服務業者聯合稽核
		推動與執行國家級漏洞獵捕(BugBounty)計畫活動
	提升中小企業資安防護	推動中小企業資安健檢團

(十)固定資產之建設改良擴充

116 年度固定資產預算編列 282,358 千元，項目包含機械及設備及什項設備，其中以機械及設備為大宗，預計依承接計畫工作項目採購網路設備、儲存設備、威脅情資研究運算等設備，資金來源為政府專案補助收入。

116 年度固定資產建設改良擴充與資金來源詳見圖 4。

圖4　116 年度固定資產建設改良擴充與資金來源



單位：新臺幣千元

建設改良擴充	116年度預算	資金來源	116年度預算
土地改良物	-	政府專案補助收入	282,358
房屋及建築	-		
機械及設備	277,358		
交通及運輸設備	-		
什項設備	5,000		
租賃權益改良	-		
合計	**282,358**	**合計**	**282,358**

(十一) 長期債務之舉借及償還

本院無。

(十二) 其他重要計畫

本院無。

四、本年度政府機關核撥經費概述

116 年度政府專案補助收入計 1,216,029 千元(經常門 909,737 千元，資本門 306,292 千元)，主要計畫項目及預算分別為：(1) 提升通傳領域資安聯防機制及強化通傳網路預警應變能力計畫 93,413 千元、(2) 資料保護驗測機制推動計畫 25,620 千元、(3) 數位政府資安生態防護推動計畫 253,350 千元、(4) 關鍵基礎設施資安防護計畫 313,200 千元、(5) AI 網路威脅偵防技術研究計畫 93,786 千元、(6) 數位訊息分析技術研發計畫 90,160 千元、(7) 中小企業及產品資安強化計畫 35,000 千元、(8) 全民資安意識與韌性延伸推動計畫 20,400 千元、(9) 政府數位韌性強化計畫 100,000 千元、(10) 國家資通安全研究院營運發展計畫 191,100 千元。

政府專案補助收入認列說明：政府補助經費合計 1,216,029 千元，扣除本年度預計執行之資本支出轉列遞延收入 306,292 千元，另增列當年度提列折舊及攤銷數轉認列收入 145,886 千元，116 年度預計認列政府專案補助收入為 1,055,623 千元。

五、近二年度預算財務自籌情形概述

本院收入結構以政府補助計畫收入為基本盤，並配合業務職掌於年度執行期間主動爭取各界委託計畫，作為自籌收入之主要來源。鑑於委託計畫除因本院執行成效良好而提升次年度續約可能性外，亦須視當年度需求積極開拓新興計畫，致使整體收益難於年度期初精準預估與明列。即便如此，本院仍展現強烈之業務拓展動能，採滾動式推動策略擴展自籌資源，期能達成自籌收入逐年穩健成長之目標。

六、本年度預算概要

(一)收支營運概況

1. 收入總額預估為 1,063,845 千元，包括業務收入 1,063,235 千元及業務外收入 610 千元。業務收入為勞務收入 200 千元、政府專案補助收入 1,055,623 千元及政府機關捐贈收入 7,412 千元。116 年度收入數較上年度減少 45,657 千元，約 4.12%。
2. 成本與費用總額預估為 1,063,645 千元，包括勞務成本 200 千元、業務費用 878,260 千元及管理及總務費用 185,185 千元。116 年度成本與費用較上年度減少 45,657 千元，約 4.12%。
3. 收支相抵後，116 年度預估賸餘 200 千元。
4. 116 年度收入、支出及餘絀詳見圖 5，最近 5 年收入與支出詳見圖 6。

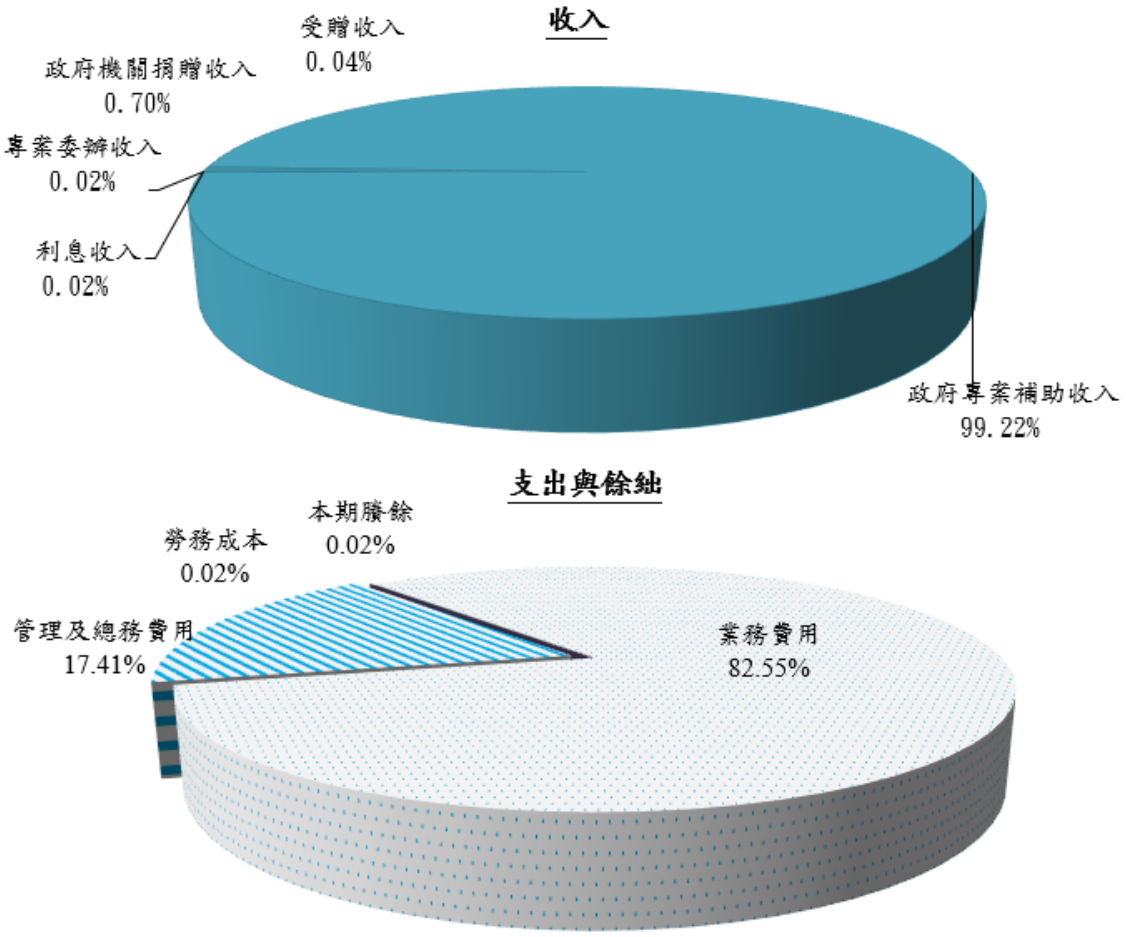
(二)淨值變動概況

本院 116 年度期初預估累計賸餘 86,269 千元，預估本年度預算為賸餘 200 千元，期末累積賸餘為 86,469 千元。

(三)現金流量概況

本院 116 年度預估業務活動之淨現金流入為 188,803 千元，投資活動之淨現金流出 306,292 千元，籌資活動之淨現金流入 148,483 千元，故本年度現金及約當現金之淨增 30,994 千元。

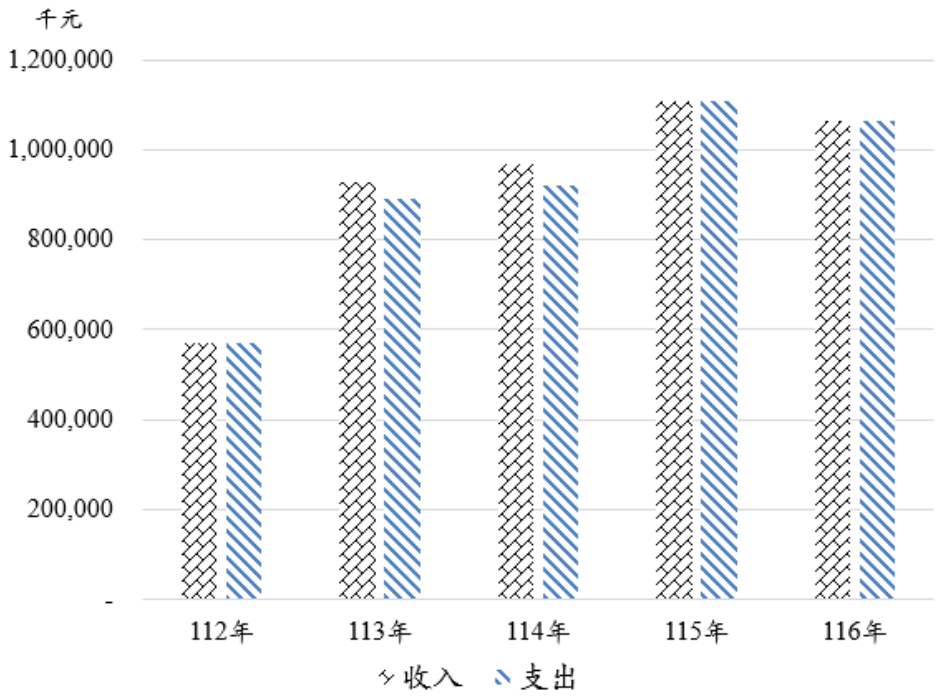
圖5　116 年度收入、支出及賸餘



單位：新臺幣千元

收入	116年度預算	支出與餘絀	116年度預算
業務收入		業務成本與費用	
專案委辦收入	200	勞務成本	200
政府機關捐贈收入	7,412	業務費用	878,260
政府專案補助收入	1,055,623	管理及總務費用	185,185
業務外收入		業務外費用	-
利息收入	200		
受贈收入	410		
		本期賸餘	200
合計	**1,063,845**	**合計**	**1,063,845**

圖6　最近 5 年收入與支出



單位：新臺幣千元

年度 項目	112年 決算	113年 決算	114年 決算	115年 預算	116年 預算
收入					
業務收入	566,378	924,478	968,166	1,108,787	1,063,235
業務外收入	2,726	3,413	1,011	715	610
收入合計	**569,104**	**927,891**	**969,177**	**1,109,502**	**1,063,845**
支出					
業務成本與費用	567,009	889,927	921,410	1,109,302	1,063,645
業務外費用	1,745	-	12	-	-
支出合計	**568,754**	**889,927**	**921,422**	**1,109,302**	**1,063,645**
本期賸餘	**350**	**37,964**	**47,755**	**200**	**200**

備註：115年度預算經立法程序公布者，為法定預算數，未完成相關程序者，為預算案數。以下各表同。

主要表

國家資通安全研究院

收支營運預計表

中華民國 116 年度

單位：新臺幣千元

前年度決算數		科目	本年度預算數		上年度預算數		比較增減(-)		說明
金額	%		金額	%	金額	%	金額	%	
969,177	**100.00**	**收入**	**1,063,845**	**100.00**	**1,109,502**	**100.00**	**(45,657)**	**(4.12)**	
968,166	**99.90**	**業務收入**	**1,063,235**	**99.94**	**1,108,787**	**99.94**	**(45,552)**	**(4.11)**	
277,584	28.64	勞務收入	200	0.02	21	0.00	179	852.38	
277,222	28.60	專案委辦收入	200	0.02	21	0.00	179	852.38	
362	0.04	其他勞務收入	-	-	-	-	-	-	
690,582	71.25	其他業務收入	1,063,035	99.92	1,108,766	99.93	(45,731)	(4.12)	
23,932	2.47	政府機關捐贈收入	7,412	0.70	16,125	1.45	(8,713)	(54.03)	
666,650	68.79	政府專案補助收入	1,055,623	99.22	1,092,641	98.48	(37,018)	(3.38)	
1,011	**0.10**	**業務外收入**	**610**	**0.06**	**715**	**0.06**	**(105)**	**(14.69)**	
465	0.05	財務收入	200	0.02	200	0.02	-	-	
465	0.05	利息收入	200	0.02	200	0.02	-	-	
-	-	兌換賸餘	-	-	-	-	-	-	
546	0.06	其他業務外收入	410	0.04	515	0.05	(105)	(20.39)	
531	0.05	受贈收入	410	0.04	515	0.05	(105)	(20.39)	
15	0.00	雜項收入	-	-	-	-	-	-	
921,422	**95.07**	**支出**	**1,063,645**	**99.98**	**1,109,302**	**99.98**	**(45,657)**	**(4.12)**	
921,410	**95.07**	**業務成本及費用**	**1,063,645**	**99.98**	**1,109,302**	**99.98**	**(45,657)**	**(4.12)**	
201,042	20.74	勞務成本	200	0.02	21	0.00	179	852.38	
201,042	20.74	服務成本	200	0.02	21	0.00	179	852.38	
578,633	59.70	業務費用	878,260	82.55	926,280	83.49	(48,020)	(5.18)	
578,633	59.70	業務費用	878,260	82.55	926,280	83.49	(48,020)	(5.18)	

國家資通安全研究院

收支營運預計表

中華民國 116 年度

單位：新臺幣千元

前年度決算數		科目	本年度預算數		上年度預算數		比較增減(-)		說明
金額	%		金額	%	金額	%	金額	%	
141,735	14.62	管理及總務費用	185,185	17.41	183,001	16.49	2,184	1.19	
141,735	14.62	管理費用及總務費用	185,185	17.41	183,001	16.49	2,184	1.19	
12	**0.00**	**業務外費用**	-	-	-	-	-	-	
12	0.00	財務費用	-	-	-	-	-	-	
12	0.00	兌換短絀	-	-	-	-	-	-	
-	-	**所得稅**	-	-	-	-	-	-	
47,755	**4.93**	**本期賸餘(短絀)**	**200**	**0.02**	**200**	**0.02**	-	-	

國家資通安全研究院

淨值變動預計表

中華民國 116 年度

單位：新臺幣千元

項目	基金			公積		累積餘絀		淨值其他項目		合計
	創立基金	捐贈基金	其他基金	資本公積	特別公積	累積賸餘	累積短絀	累積其他綜合餘絀	未認列為退休金成本之淨短絀	
本年度期初餘額	-	-	-	-	-	86,269	-	-	-	86,269
本年度增(減)數	-	-	-	-	-	200	-	-	-	200
本年度期末餘額	-	-	-	-	-	86,469	-	-	-	86,469

國家資通安全研究院

現金流量預計表

中華民國 116 年度

單位：新臺幣千元

項目	預算數	說明
業務活動之現金流量		
本期賸餘(短絀)	200	
利息股利之調整		
利息收入	(200)	
未計利息股利之本期賸餘(短絀)	-	
調整項目		
折舊費用	129,463	
各項攤提	24,754	
應收款項	-	
預付款項	4,618	
應付款項	29,768	
預收款項	-	
未計利息股利之現金流入(流出)	188,603	
收取利息	200	
業務活動之淨現金流入(流出)	**188,803**	
投資活動之現金流量		
增加不動產、廠房及設備	(282,358)	詳固定資產建設改良擴充明細表。
增加無形資產	(23,934)	詳無形資產明細表。
投資活動之淨現金流入(流出)	**(306,292)**	
籌資活動之現金流量		
增加遞延負債	153,908	
減少長期負債	-	
減少什項負債	(5,425)	
籌資活動之淨現金流入(流出)	**148,483**	
現金及約當現金之淨增(淨減)	**30,994**	
期初現金及約當現金	**688,402**	
期末現金及約當現金	**719,396**	

明細表

國家資通安全研究院

勞務收入明細表

中華民國 116 年度

單位：新臺幣千元

科目及營運項目	本年度預算數	說明
業務收入		
勞務收入	200	
專案委辦收入	200	資本門提列攤銷 200 千元，將遞延收入轉列專案委辦收入
總計	**200**	

國家資通安全研究院

其他業務收入明細表

中華民國116年度

單位：新臺幣千元

科目及營運項目	本年度預算數	說明
業務收入		
其他業務收入	1,063,035	
政府機關捐贈收入	7,412	資本門提列折舊及攤銷 7,412 千元，將遞延收入轉列政府機關捐贈收入。
政府專案補助收入	1,055,623	1. 數位發展部補助收入，包含： (1) 辦理「提升通傳領域資安聯防機制及強化通傳網路預警應變能力計畫」57,351 千元。 (2) 辦理「資料保護驗測機制推動計畫」22,620 千元。 2. 資通安全署補助收入，包含： (1) 辦理「數位政府資安生態防護推動計畫」192,410 千元。 (2) 辦理「關鍵基礎設施資安防護計畫」272,590 千元。 (3) 辦理「AI 網路威脅偵防技術研究計畫」63,786 千元。 (4) 辦理「數位訊息分析技術研發計畫」73,660 千元。 (5) 辦理「中小企業及產品資安強化計畫」34,385 千元。 (6) 辦理「全民資安意識與韌性延伸推動計畫」15,700 千元。 (7) 辦理「政府數位韌性強化計畫」15,000 千元。 (8) 辦理「國家資通安全研究院營運發展計畫」162,235 千元。 3. 資本門提列折舊及攤銷 145,886 千元，將遞延收入轉列政府專案補助收入。
總計	**1,063,035**	

國家資通安全研究院

財務收入明細表

中華民國 116 年度

單位：新臺幣千元

科目及營運項目	本年度預算數	說明
業務外收入		
財務收入	200	
利息收入	200	金融機構存款利息。
總計	**200**	

國家資通安全研究院

其他業務外收入明細表

中華民國 116 年度

單位：新臺幣千元

科目及營運項目	本年度預算數	說明
業務外收入		
其他業務外收入	410	
受贈收入	410	資本門提列折舊及攤銷 410 千元，將遞延收入轉列受贈收入。
總計	**410**	

國家資通安全研究院

勞務成本明細表

中華民國 116 年度

單位：新臺幣千元

前年度決算數	上年度預算數	科目及營運項目	本年度預算數
82,291	-	**用人費用**	-
54,593	-	薪資	-
1,671	-	加(夜)班費	-
1,028	-	津貼	-
14,449	-	獎金	-
3,360	-	退休及卹償金	-
7,190	-	福利費	-
85,021	-	**服務費用**	-
1,013	-	水電費	-
1,551	-	郵電費	-
4,859	-	旅運費	-
506	-	印刷裝訂及公告費	-
4,057	-	修理保養及保固費	-
37	-	保險費	-
12,784	-	一般服務費	-
60,214	-	專業服務費	-
-	-	公關慰勞費	-
731	-	**材料及用品費**	-
-	-	使用材料費	-
731	-	用品消耗	-

國家資通安全研究院

勞務成本明細表

中華民國 116 年度

單位：新臺幣千元

前年度決算數	上年度預算數	科目及營運項目	本年度預算數
2,981	**-**	**租金與利息**	**-**
684	-	地租及水租	-
1,889	-	房租	-
54	-	機器租金	-
17	-	交通及運輸設備租金	-
337	-	什項設備租金	-
123	**21**	**折舊、折耗及攤銷**	**200**
102	-	不動產、廠房及設備折舊	179
21	21	攤銷	21
-	**-**	**稅捐與規費(強制費)**	**-**
-	-	消費與行為稅	-
-	-	規費	-
937	**-**	**會費、捐助、補助、分攤、救助（濟）與交流活動費**	**-**
-	-	會費	-
125	-	捐助、補助與獎助	-
812	-	分擔	-
28,958	**-**	**其他**	**-**
28,958	-	其他費用	-
201,042	**21**	**合計**	**200**

國家資通安全研究院

勞務成本說明

中華民國 116 年度

科目及營運項目	說　　明
折舊、折耗及攤銷	1. 折舊：依行政院訂頒「財物標準分類」之使用年限，採直線法提列，預計 179 千元，詳見資產折舊明細表。 2. 攤銷：電腦軟體等無形資產攤銷預計 21 千元，詳見無形資產攤銷明細表。

國家資通安全研究院

業務費用明細表

中華民國 116 年度

單位：新臺幣千元

前年度決算數	上年度預算數	科目及營運項目	本年度預算數
250,034	**442,739**	**用人費用**	**455,683**
164,700	296,273	薪資	309,279
8,423	10,407	加(夜)班費	12,744
1,797	-	津貼	739
42,746	76,969	獎金	71,753
9,872	18,318	退休及卹償金	19,327
22,496	40,772	福利費	41,841
237,934	**332,729**	**服務費用**	**227,576**
3,018	5,705	水電費	5,018
23,910	22,376	郵電費	25,911
10,272	50,871	旅運費	32,554
346	2,106	印刷裝訂及公告費	1,316
8,321	9,501	修理保養及保固費	13,419
37	150	保險費	100
53,119	44,814	一般服務費	54,061
138,911	197,206	專業服務費	94,997
-	-	公關慰勞費	200
1,750	**6,052**	**材料及用品費**	**3,420**
-	2,559	使用材料費	156
1,750	3,493	用品消耗	3,264
5,097	**28,860**	**租金與利息**	**25,096**
1,217	905	地租及水租	1,217
3,547	27,655	房租	15,274

國家資通安全研究院

業務費用明細表

中華民國 116 年度

單位：新臺幣千元

前年度決算數	上年度預算數	科目及營運項目	本年度預算數
82	100	機器租金	150
75	-	交通及運輸設備租金	500
176	200	什項設備租金	7,955
62,063	**99,818**	**折舊、折耗及攤銷**	**145,886**
50,045	82,361	不動產、廠房及設備折舊	122,514
12,018	17,457	攤銷	23,372
-	**100**	**稅捐與規費(強制費)**	**-**
-	50	消費與行為稅	-
-	50	規費	-
2,838	**11,830**	**會費、捐助、補助、分攤、救助（濟）與交流活動費**	**9,381**
121	240	會費	125
288	-	捐助、補助與獎助	-
2,429	11,140	分擔	5,470
-	450	補貼(償)、獎勵、慰問與救助(濟)	-
-	-	競賽及交流活動費	3,786
18,917	**4,152**	**其他**	**11,218**
18,917	4,152	其他費用	11,218
578,633	**926,280**	**合計**	**878,260**

國家資通安全研究院

業務費用說明

中華民國 116 年度

科目及營運項目	說　　明
用人費用	正式人員之薪資、獎金、退休金及卹償金、以及保險等費用，預計 455,683 千元。
服務費用	1. 水電費：辦公室水電費預計 5,018 千元。 2. 郵電費：網路費、電話費預計 25,911 千元。 3. 旅運費：國內外出差等相關費用及運費預計 32,554 千元。 4. 印刷裝訂及公告費：業務推廣之印刷品與宣導費等費用預計 1,316 千元。 5. 修理保養及保固費：資訊設備修繕養護費預計 13,419 千元。 6. 保險費：機械、設備保險費及各項活動意外責任險等預計 100 千元。 7. 一般服務費：勞務工作委外外包費、學研合作技術開發費用、計時及計件人員酬金預計 54,061 千元。 8. 專業服務費：電腦軟體授權費、雲端服務費用、委託資安相關之專業機構及國內外學者專家提供服務及諮詢之費用及派員參加國內訓練費用及各式講座鐘點費等預計 94,997 千元。 9. 公關慰勞費：因應業務推廣需要之公關費預計 200 千元。
材料及用品費	1. 使用材料費：設備運轉維護所耗用之物料預計 156 千元。 2. 用品消耗：辦公事務用品等消耗品及非消耗品及資安相關標準、國內外期刊預計 3,264 千元。
租金與利息	1. 辦公處所租金及各項活動場地租金預計 16,491 千元。 2. 業務所需之機器、交通及運輸、什項設備等租金預計 8,605 千元。
折舊、折耗及攤銷	1. 折舊：依行政院訂頒「財物標準分類」之使用年限，採直線法提列，預計 122,514 千元，詳見資產折舊明細表。 2. 攤銷：電腦軟體等無形資產攤銷預計 23,372 千元，詳見無形資產攤銷明細表。
會費、捐助、補助、分攤、救助（濟）與交流活動費	1. 參加國內外組織會費 125 千元。 2. 分擔辦公處所大樓管理費用預計 5,470 千元。 3. 參加競賽及交流活動費用預計 3,786 千元。
其他費用	辦理各項活動、演練及研討會等之會議費用及其他 11,218 千元。

國家資通安全研究院

管理及總務費用明細表

中華民國 116 年度

單位：新臺幣千元

前年度決算數	上年度預算數	科目及營運項目	本年度預算數
72,470	**78,147**	**用人費用**	**91,156**
47,133	52,262	薪資	61,869
2,737	4,263	加(夜)班費	2,549
576	-	津貼	148
12,565	12,502	獎金	14,354
2,918	3,213	退休及卹償金	3,866
6,541	5,907	福利費	8,370
42,758	**77,487**	**服務費用**	**69,184**
927	967	水電費	1,020
1,405	7,145	郵電費	1,550
404	1,904	旅運費	445
351	535	印刷裝訂及公告費	386
13,261	14,097	修理保養及保固費	14,587
158	162	保險費	173
5,909	6,289	一般服務費	6,500
20,081	45,838	專業服務費	44,073
262	550	公關慰勞費	450
661	**1,852**	**材料及用品費**	**729**
21	-	使用材料費	135
640	1,852	用品消耗	594
1,111	**4,877**	**租金與利息**	**5,137**
-	60	地租及水租	-
1,077	4,617	房租	5,100

國家資通安全研究院

管理及總務費用明細表

中華民國 116 年度

單位：新臺幣千元

前年度決算數	上年度預算數	科目及營運項目	本年度預算數
-	-	機器租金	-
-	-	交通及運輸設備租金	-
34	200	什項設備租金	37
23,413	**17,707**	**折舊、折耗及攤銷**	**8,131**
19,181	14,097	不動產、廠房及設備折舊	6,770
4,232	3,610	攤銷	1,361
28	**410**	**稅捐與規費(強制費)**	**64**
28	50	消費與行為稅	31
-	360	規費	33
703	**1,987**	**會費、捐助、補助、分攤、救助（濟）與交流活動費**	**784**
-	12	會費	10
-	-	捐助、補助與獎助	-
703	1,975	分擔	774
590	**534**	**其他**	**10,000**
590	534	其他費用	10,000
141,734	**183,001**	**合計**	**185,185**

國家資通安全研究院

管理及總務費用說明

中華民國 116 年度

科目及營運項目	說　　明
用人費用	正式人員之薪資、獎金、退休金及卹償金、以及保險等費用，預計 91,156 千元。
服務費用	1. 水電費：辦公室水電費預計 1,020 千元。 2. 郵電費：公務信件寄送費、電話及網路費預計 1,550 千元。 3. 旅運費：國內外出差、出國考察交通費及生活費等費用預計 445 千元。 4. 印刷裝訂及公告費：徵才刊登及各式書表報告之印刷費預計 386 千元。 5. 修理保養及保固費：辦公設備、房屋與交通及運輸設備修繕養護費預計 14,587 千元。 6. 保險費：財產保險費與建物火險費預計 173 千元。 7. 一般服務費：勞務工作委外外包、計時人員酬金等費用預計 6,500 千元。 8. 專業服務費：電腦軟體授權費、雲端服務費用、派員參加國內外訓練費用及各式講座鐘點費等預計 44,073 千元。 9. 公關慰勞費：因應業務推廣需要之公關費預計 450 千元。
材料及用品費	1. 使用材料費：設備運轉維護所耗用之物料預計 135 千元。 2. 用品消耗：辦公事務用品等消耗品及非消耗品預計 594 千元。
租金與利息	1. 房租：辦公處所租金費用預計 5,100 千元。 2. 什項設備租金：維運所需之機器設備、電信機櫃租用費用租金、辦公事務影印機及活動硬體等設備租賃費用預計 37 千元。
折舊、折耗及攤銷	1. 折舊：依行政院訂頒「財物標準分類」之使用年限，採直線法提列，預計 6,770 千元，詳見資產折舊明細表。 2. 攤銷：電腦軟體等無形資產攤銷預計 1,361 千元，詳見無形資產攤銷明細表。
稅捐與規費(強制費)	1. 消費與行為稅：車輛使用牌照稅及其他預計 31 千元。 2. 規費：政府機關各項規費費用預計 33 千元。
會費、捐助、補助、分攤、救助（濟）與交流活動費	1. 參加國內外組織會費 10 千元。 2. 分擔：分擔辦公處所大樓管理費用預計 774 千元。
其他費用	辦理各項活動等之會議費用及其他預計 10,000 千元。

國家資通安全研究院

無形資產明細表

中華民國 116 年度

單位：新臺幣千元

項目	本年度預算數	說明
電腦軟體	**23,934**	本年度新增電腦軟體及可資本化授權，包含雲端軟體、Xensor 行動版端點惡意程式檢測工具、Veeam 3 年授權訂閱服務、海纜圖層展示平臺、C-NOC 平臺改版、VMware 授權、端點防護平臺、GeoIP2 Databases 及 Open Text SMA 等。
合計	**23,934**	

國家資通安全研究院

固定資產建設改良擴充明細表

中華民國 116 年度

單位：新臺幣千元

項目	本年度預算數	說明
不動產、廠房及設備		
機械及設備	277,358	執行業務所需資訊電腦設備，包含伺服器、高效能人工智慧運算設備、數位訊息威脅情資研究運算設備、資料蒐集伺服器、GPU 運算主機、機架型伺服器、筆記型電腦、會議資訊設備及檢測設備等。
什項設備	5,000	辦理網路與通訊韌性建置所需設備，包含入侵防禦設備、網路交換器、防火牆、無線 AP、控制器、PoE 交換器、高頻寬光纖網路、光模組、結構化布線、OOB 管理設備、PDU/UPS、機房環境監控及相關告警硬體等。
合計	**282,358**	

國家資通安全研究院

無形資產攤銷明細表

中華民國 116 年度

單位：新臺幣千元

項目	本年度預算數	說明
電腦軟體		
前年度決算資產原值	**92,065**	
上年度預計新增資產原值	**25,990**	
本年度預計新增資產原值	**23,934**	本年度新增電腦軟體及可資本化授權，包含雲端軟體、Xensor 行動版端點惡意程式檢測工具、Veeam 3 年授權訂閱服務、海纜圖層展示平臺、C-NOC 平臺改版、VMware 授權、端點防護平臺、GeoIP2 Databases 及 Open Text SMA 等。
本年度(12 月底)止資產總額	**141,989**	
本年度應提攤銷額	**24,754**	
勞務成本	21	
業務費用	23,372	
管理及總務費用	1,361	

說明：112 年度攤銷額 476 千元

113 年度攤銷額 9,242 千元

114 年度攤銷額 16,271 千元

115 年度攤銷額 20,961 千元

國家資通安全研究院

資產折舊明細表

中華民國 116 年度

單位：新臺幣千元

項目	不動產、廠房及設備							其他	合計
	土地改良物	房屋及建築	機械及設備	交通及運輸設備	什項設備	租賃資產	租賃權益改良		
前年度決算資產原值	**-**	**-**	**348,251**	**3,015**	**3,996**	**2,184**	**23,673**	**17,761**	**398,880**
上年度預計增(減)資產原值	**-**	**-**	**80,479**	**13,200**	**-**	**-**	**48,125**	**(17,761)**	**124,043**
本年度預計增(減)資產原值	**-**	**-**	**277,358**	**-**	**5,000**	**-**	**-**		**282,358**
資產重估增值額	**-**	**-**	**-**	**-**	**-**	**-**	**-**		**-**
本年度(12 月底)止資產總額	**-**	**-**	**706,088**	**16,215**	**8,996**	**2,184**	**71,798**	**-**	**805,281**
本年度應提折舊額	**-**	**-**	**112,520**	**2,057**	**779**	**-**	**14,107**		**129,463**
勞務成本	-	-	162	-	17	-	-		179
業務費用	-	-	105,926	2,007	697	-	13,884		122,514
管理及總務費用	-	-	6,432	50	65	-	223		6,770

本頁空白

參考表

國家資通安全研究院

預計平衡表

中華民國 116 年度

單位：新臺幣千元

114 年(前年) 12 月 31 日 實際數	科目	116 年 12 月 31 日 預計數	115 年(上年) 12 月 31 日 預計數	比較增減(-)
	資產			
506,805	**流動資產**	**719,396**	**693,020**	**26,376**
277,126	現金	719,396	688,402	30,994
277,126	銀行存款	719,396	688,402	30,994
174,899	應收款項	-	-	-
174,839	應收帳款	-	-	-
60	其他應收款	-	-	-
54,780	預付款項	-	4,618	(4,618)
73	用品盤存	-	44	(44)
54,467	預付費用	-	-	-
240	其他預付款	-	4,574	(4,574)
263,685	**不動產、廠房及設備**	**467,283**	**314,388**	**152,895**
348,247	機械及設備	706,088	428,730	277,358
(108,475)	減：累計折舊	(301,553)	(189,033)	(112,520)
3,015	交通及運輸設備	16,215	16,215	-
(1,031)	減：累計折舊	(6,024)	(3,967)	(2,057)
3,996	什項設備	8,996	3,996	5,000
(1,302)	減：累計折舊	(2,827)	(2,048)	(779)
2,184	租賃資產	2,184	2,184	-
(1,802)	減：累計折舊	(2,184)	(2,184)	-
23,673	租賃權益改良	71,798	71,798	-
(4,820)	減：累計折舊	(25,410)	(11,303)	(14,107)
66,076	**無形資產**	**70,285**	**71,105**	**(820)**
66,076	無形資產	70,285	71,105	(820)
66,076	電腦軟體	70,285	71,105	(820)
33,278	**其他資產**	**10,776**	**10,776**	**-**
33,278	什項資產	10,776	10,776	-

國家資通安全研究院

預計平衡表

中華民國 116 年度

單位：新臺幣千元

114 年(前年) 12 月 31 日 實際數	科目	116 年 12 月 31 日 預計數	115 年(上年) 12 月 31 日 預計數	比較增減(-)
14,440	存出保險金	10,776	10,776	-
1,077	暫付及待結轉帳項	-	-	-
17,761	代管資產	-	-	-
869,844	**資產合計**	**1,267,740**	**1,089,289**	**178,451**
	負債			
407,946	**流動負債**	**430,335**	**400,567**	**29,768**
406,470	應付款項	430,335	400,567	29,768
315,733	應付帳款	344,228	319,332	24,896
79,642	應付費用	86,107	81,235	4,872
11,095	其他應付款	-	-	-
1,476	預收款項	-	-	-
1,476	預收收入	-	-	-
220	**長期負債**	**-**	**-**	**-**
220	應付租賃款	-	-	-
375,609	**其他負債**	**750,936**	**602,453**	**148,483**
326,374	遞延負債	732,905	578,997	153,908
326,374	遞延收入	732,905	578,997	153,908
49,235	什項負債	18,031	23,456	(5,425)
31,474	存入保證金	18,031	23,456	(5,425)
-	暫收及待結轉帳項	-	-	-
17,761	應付代管資產	-	-	-
783,775	**負債合計**	**1,181,271**	**1,003,020**	**178,251**
	淨值			
86,069	**累積餘絀**	**86,469**	**86,269**	**200**
86,069	累積賸餘	86,469	86,269	200
86,069	**淨值合計**	**86,469**	**86,269**	**200**
869,844	**負債及淨值合計**	**1,267,740**	**1,089,289**	**178,451**

國家資通安全研究院

5 年來主要營運項目分析表

中華民國 116 年度

單位：新臺幣千元

年度與項目	單位	數量	單位成本(元) 或 平均利(費)率	預(決)算數	說明
本年度預算數				**1,063,645**	本院主要營運項目為執行政府專案補助計畫及專案委辦計畫，無法明確計算單位成本，故以全年度營運所需經費預算表達。
勞務成本				200	
業務費用				878,260	
管理及總務費用				185,185	
上年度預算數				**1,109,302**	
勞務成本				21	
業務費用				926,280	
管理及總務費用				183,001	
前年度決算數				**921,410**	
勞務成本				201,042	
業務費用				578,633	
管理及總務費用				141,735	
113 年度決算數				**889,927**	
勞務成本				104,782	
業務費用				613,338	
管理及總務費用				171,807	
112 年度決算數				**567,008**	
業務費用				439,128	
管理及總務費用				127,880	

國家資通安全研究院

員工人數彙計表

中華民國 116 年度

單位：人

職類(稱)	本年度員額預計數	說明
正式人員	319	116 年度預計員額 319 人。
合計	**319**	

國家資通安全研究院

用人費用彙計表

中華民國 116 年度

單位：新臺幣千元

科目	本年度預算數	說明
薪資	371,148	正式人員 319 名薪資。
超時工作報酬	15,293	延長工時加班費、輪值及未休假加班費。
津貼	887	外勤津貼。
獎金	86,107	績效獎金、考績獎金與年終獎金。
退休及卹償金	23,193	退休及卹償金等。
福利費	50,211	雇主負擔之勞健保、團保及旅遊補助等福利費用。
合計	**546,839**	

國家資通安全研究院

各項費用彙計表

中華民國 116 年度

單位：新臺幣千元

前年度決算數	上年度預算數	科目	本年度預算數			
			合計	勞務成本	業務費用	管理及總務費用
404,795	**520,886**	**用人費用**	**546,839**	**-**	**455,683**	**91,156**
266,426	348,535	薪資	371,148	-	309,279	61,869
12,831	14,670	加(夜)班費	15,293	-	12,744	2,549
3,401	-	津貼	887	-	739	148
69,760	89,471	獎金	86,107	-	71,753	14,354
16,150	21,531	退休及卹償金	23,193	-	19,327	3,866
36,227	46,679	福利費	50,211	-	41,841	8,370
365,713	**410,216**	**服務費用**	**296,760**	**-**	**227,576**	**69,184**
4,959	6,672	水電費	6,038	-	5,018	1,020
26,867	29,521	郵電費	27,461	-	25,911	1,550
15,535	52,775	旅運費	32,999	-	32,554	445
1,203	2,641	印刷裝訂及公告費	1,702	-	1,316	386
25,639	23,598	修理保養及保固費	28,006	-	13,419	14,587
231	312	保險費	273	-	100	173
71,811	51,103	一般服務費	60,561	-	54,061	6,500
219,206	243,044	專業服務費	139,070	-	94,997	44,073
262	550	公關慰勞費	650	-	200	450
3,142	**7,904**	**材料及用品費**	**4,149**	**-**	**3,420**	**729**
21	2,559	使用材料費	291	-	156	135
3,121	5,345	用品消耗	3,858	-	3,264	594
9,189	**33,737**	**租金與利息**	**30,233**	**-**	**25,096**	**5,137**
1,901	965	地租及水租	1,217	-	1,217	-
6,513	32,272	房租	20,374	-	15,274	5,100
136	100	機器租金	150	-	150	-
92	-	交通及運輸設備租金	500	-	500	-
547	400	什項設備租金	7,992	-	7,955	37

國家資通安全研究院

各項費用彙計表

中華民國 116 年度

單位：新臺幣千元

前年度決算數	上年度預算數	科目	本年度預算數			
			合計	勞務成本	業務費用	管理及總務費用
85,600	**117,546**	**折舊、折耗及攤銷**	**154,217**	**200**	**145,886**	**8,131**
69,329	96,458	不動產、廠房及設備折舊	129,463	179	122,514	6,770
16,271	21,088	攤銷	24,754	21	23,372	1,361
28	**510**	**稅捐與規費(強制費)**	**64**	**-**	**-**	**64**
28	100	消費與行為稅	31	-	-	31
-	410	規費	33	-	-	33
4,478	**13,817**	**會費、捐助、補助、分攤、救助（濟）與交流活動費**	**10,165**	**-**	**9,381**	**784**
121	252	會費	135	-	125	10
413	-	捐助、補助與獎助	-	-	-	-
3,944	13,115	分擔	6,244	-	5,470	774
-	450	補貼(償)、獎勵、慰問與救助(濟)	-	-	-	-
-	-	競賽及交流活動費	3,786	-	3,786	-
12	-	**短絀、賠償與保險給付**	-	-	-	-
12	-	各項短絀	-	-	-	-
48,465	**4,686**	**其他**	**21,218**	**-**	**11,218**	**10,000**
48,465	4,686	其他費用	21,218	-	11,218	10,000
921,422	**1,109,302**	**總計**	**1,063,645**	**200**	**878,260**	**185,185**

國家資通安全研究院
公務車輛明細表
中華民國 116 年度

單位：新臺幣千元

車輛數	車輛種類	乘客數量(不含司機)	購置年月	汽缸總排氣量(立方公分)	油料費(全年)			養護費	其他	備註
					數量(公升)	單價(元)	金額			
1	小客車	4	112.05	1,798	575	33	19	26	14	車號:CEM-0792
1	小客車	4	112.05	1,798	575	33	19	26	14	車號:CEM-0793
2	合計				1,150	33	38	52	28	

附錄

國家資通安全研究院

立法院審議行政法人預算所提決議及附帶決議辦理情形報告表

中華民國 115 年度

決議及附帶決議		辦理情形
項次	內容	
	一、通案決議部分： 無。 二、各委員會審查決議部分： 無。	

本頁空白