國家資通安全研究院

114年度業務計畫

中華民國113年8月

目次

圖目次

表目次

壹、前言

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、願景與目標

(一) 本院核心價值與願景

本院為國家級研究機構，以「打造國際級資安韌性科研團隊，建立安全、安心及安穩的數位環境」為願景，專注國家整體資安防護科研及服務工作，面對外部資安威脅及與日俱增之駭侵趨勢，協助公私部門加速建構完善之資安環境，落實資安管理，帶動整體資安產業向上發展，以達成「強化國家資安防護機制，提升智慧國家資安韌性」、「建立國家級資安團隊，確保數位國土安全」、「推動資安技術研發，促進產業資安發展」等 3 大目標。

本院結合各界力量推動資通安全科技研究及應用發展、協處國家資通安全防護機制及關鍵基礎設施防護、培訓資通安全人才、推廣全民資安意識、策進產學服務及國際合作，確保民眾數位生活福祉，提升國家數位韌性，本院 5 大核心價值(START)及推動策略如下，發展藍圖詳見圖 1。

1. 安全(Security)：建構資安防護聯網，強化資安預警能量。
2. 技術(Technology)：研發資安前瞻技術，帶動自主創研能量。
3. 主動(proActiveness)：觀測各國資安情勢，深化國際合作交流。
4. 韌性(Resilience)：推動公私協同治理，提升關鍵設施韌性。
5. 信賴(Trust)：培育資安實戰人才，推廣全民資安意識。

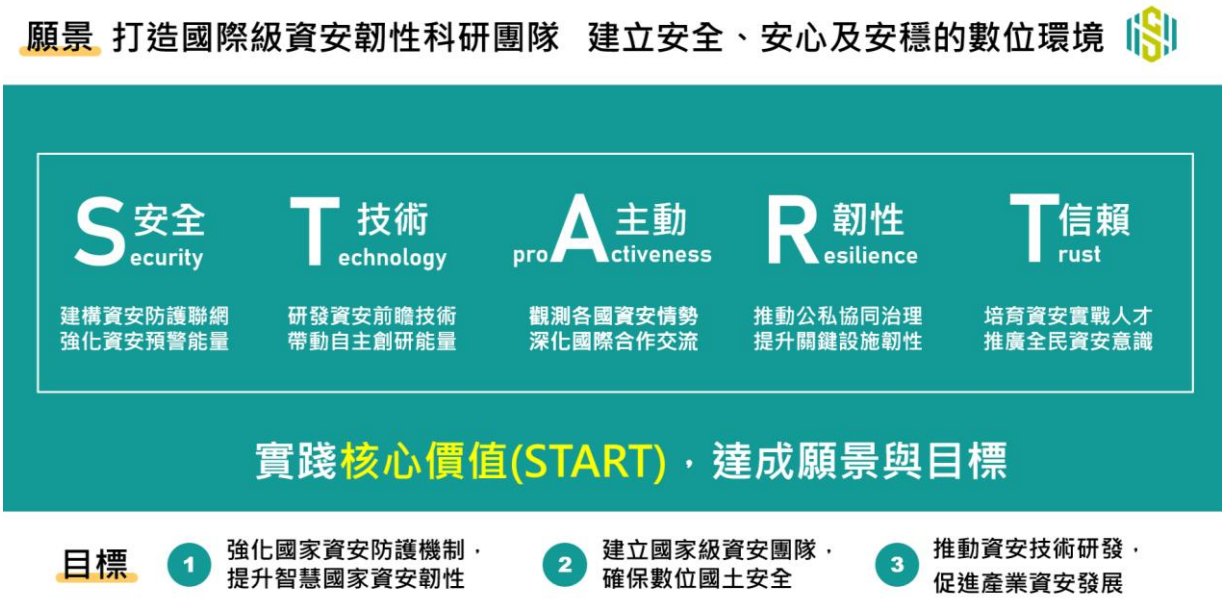

圖1　國家資通安全研究院發展藍圖

(二) 國家政策與 114 年資安院業務推動目標

本院願景目標與國家層級政策緊密整合，以「打造國際級資安韌性科研團隊，建立安全、安心及安穩的數位環境」作為願景，以確保與國家資通安全發展方案中「打造堅韌安全之智慧國家」的目標一致，並同時呼應《資安即國安》戰略報告中建構「堅韌、安全、可信賴的智慧國家」之遠景，我國資安政策與本院重點業務整合架構詳見圖 2。

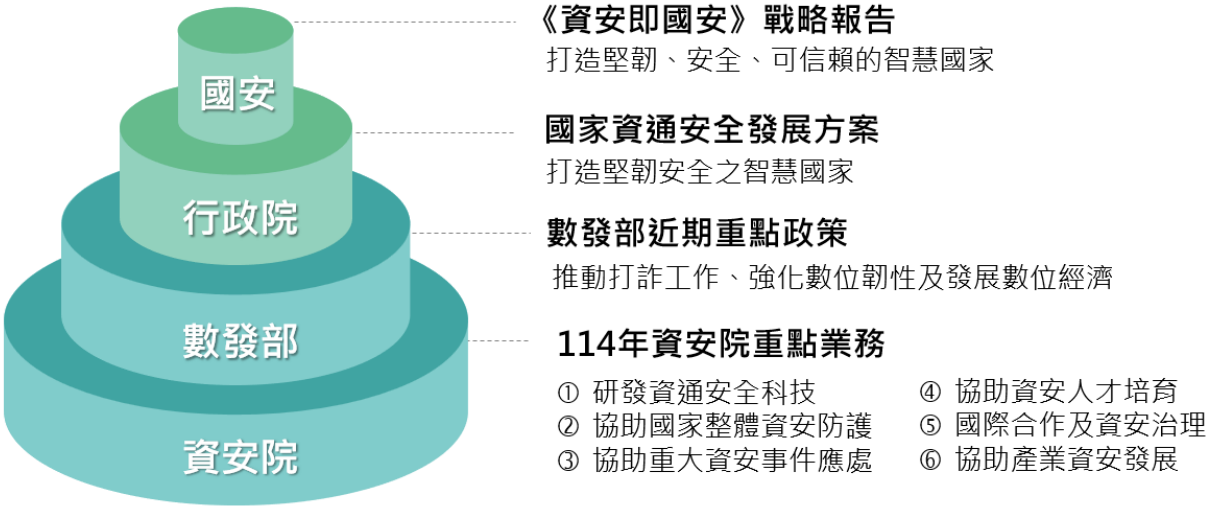

圖2　資安政策與重點業務整合架構

為協助數發部落實「推動打詐工作」、「強化數位韌性」及「發展數位經濟」政策推動方向，本院設定「強化國家資安防護機制，提升智慧國家資安韌性」、「建立國家級資安團隊，確保數位國土安全」及「推動資安技術研發，促進產業資安發展」等 3 大目標(Objectives)，並運用前述策略，設定價值導向項目標關鍵成果(Key Results)，化為具體重點業務推動計畫，支持國家資安政策與實踐資安院任務使命。

本院整合國家層級政策方向與目標，規劃 114 年重點業務推動計畫，並積極爭取相關預算支應，將本院願景與使命轉化為具體可執行之行動方案，協助政府建構國家級資安防護體系，從研發前瞻資通安全科技到培育專業人才，全面提升國家資安量能，為我國資安發展奠定堅實基礎。

(一) 研發資通安全科技

為提升國家資安防護能力，本院致力於資通安全科技研發及技術移轉與創新育成。科技研發方面，發展 AI 網路主動式防禦技術，開發智慧分析與追蹤技術，包括威脅態勢預警與攻擊來源鑑別等。針對資料隱私保護與加值應用，本院亦積極發展隱私保護前瞻研究，並擴展隱私強化技術應用，投入差分隱私、合成資料等先進技術之開發與應用。此外，配合國家政策任務，將運用 AI 技術提升防詐能力，因應不斷變化之詐騙挑戰，保障民眾資訊與財產安全。

(二) 協助國家整體資安防護

為強化國家整體資安防護，於政府網路資安縱深防護，定期執行網路攻防演練、建立關鍵基礎設施攻防演練場域、開展駭侵研析與偵測防護工作。同時亦推動政府領域聯防監控及資安防禦向上集中，包含端點偵測、誘捕偵測及黑名單自動化阻擋等措施。

針對協助政府機關強化主動防禦能力，本院推動零信任網路資安防護，透過制定相關指引與評估工具協助機關導入零信任機制。本院

自 113 年起接手維運國家通訊暨網際安全中心(NCCSC)，未來將持續協助完善通傳領域關鍵基礎設施監督管理，強化通傳網路資安監控、分析、通報及應處能力。

(三) 協助重大資安事件應處

本院長期協助政府機關應對重大資安事件，因應近年來個資外洩事件增加，針對重大矚目個資外洩事件，本院提供即時行政檢查作業技術支援。透過資安通報與諮詢服務，協助機關及時處理資安事件。由專業技術團隊提供事件處理與鑑識分析服務，包括遠端與現場鑑識，以評估影響、查找根因並提出改善建議。駭侵研析方面，分析惡意程式樣本，萃取攻擊特徵，部署偵測規則，並追蹤攻擊族群，全面強化國家資訊網路防護能力。

(四) 協助資安人才培育

為協助培育資安人才，本院深入研究資安現況，以準確掌握目標族群需求，作為後續輔導方案參考，並依據研究結果，編製適合之資安培訓教材，確保內容實用且易於理解，滿足不同組織具體需求。成立微型企業資安服務團，為中小型企業、非政府組織等提供實地輔導，解決所面臨之資安難題，並積極與大專院校合作，開設實務課程，培養具備實戰經驗之資安人才。另外，為擴大影響力，將整合公私資源舉辦多元化推廣活動，全面提升公眾資安意識。

(五) 國際合作及資安治理

持續研析「資通安全管理法」發展動向，並參考國際趨勢制定適切之資安參考指引。推動 IT 與 OT 資安治理成熟度評估，深入研究國際關鍵基礎設施防護策略，作為我國防護策略之參考。本院亦協助建立國家層級資安風險評估機制，精準掌握關鍵基礎設施面臨之資安威脅與風險，為決策提供可靠依據。

國際合作領域，積極參與 FIRST、APCERT 及 APEC TEL 等重要

國際組織，持續擴大我國國際影響力，透過建立雙邊或多邊合作關係，積極參與跨國資安演練，不斷強化國際資安聯防能力。同時，與國外頂尖機構開展深度合作，顯著提升資安技術研發實力。

定期發布資通安全技術年報與國際資安政策觀測，分析全球資安威脅趨勢及重大事件，提供制定國家資安策略之關鍵參考。提供全面且與國際接軌的資安治理體系，為國家於數位時代之安全與發展奠定堅實基礎。

(六) 協助產業資安發展

為強化企業資安防護，本院自 113 年承接台灣電腦網路危機處理暨協調中心(TWCERT/CC)，並透過「擴大推廣會員服務」、「提高主動通報誘因」、「結合行政指導擴展」、「強化公私鏈結聯防」及「深化國際合作交流」等 5 大策略運營 TWCERT/CC，全面提升企業資安防護能力。從即時預警到事件處理，國內聯防到國際合作，完整建構企業資安支持體系。設立企業資安事件通報窗口，為中小企業提供專業應變建議與技術協助，通過提供多元化服務與建立合作方式，協助企業應對日益複雜之資安威脅，增強整體產業競爭力。

貳、年度工作計畫

為實現規劃之 114 年重點業務推動計畫，本院積極爭取政府與民間委託專案，已爭取之政府補助與自籌計畫說明如下。

一、政府資通安全防護工作執行計畫

協助數位發展部資通安全署(以下簡稱資安署)執行國家資安防禦相關作業，包含資安署「臺灣資安卓越深耕-資安卓越中心計畫」與「整體政府資通安全防禦技術暨系統韌性強化計畫」之執行工項，並符合其績效指標。

(一) 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，培訓國內實戰人才，課程對象以具本國籍且擁有 2 年以上資安實務職場經驗之企業、法人與政府機構之資安資深人員為主。

(二) 推動公私協同治理

1. 研析及建議調適資通安全管理法及子法

考量國家資安戰略需求、資通安全管理法推動執行情形及技術與國際關係等外在環境之變化，研析並提出資通安全管理法之發展建議，協助權責機關調適法制內容並擘劃推進策略。

2. 研發制定資安參考指引

因應國際資安威脅趨勢與新興科技發展，以及國際資安標準或我國法制規範作業等因素，定期檢視資安相關規範之整體發展藍圖，視實際需要增修藍圖內容，並依規劃時程編撰或修訂資安相關參考指引。

3. 提供政府機關(構)專業化資安技術檢測服務

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，針對終端設備、網路架構、網域主機、資通系統及資料庫等構面執行檢測，找出潛在資安風險，並針對檢測結果提供改善建議，以協助強化受測單位資安防護能力。

4. 指派專業資安稽核人員協助年度稽核作業

配合資安署 114 年資通安全稽核計畫與相關重大專案需求，支援熟稔資安法規與具資安稽核能力或經驗之人員擔任稽核委員，配合執行實地稽核作業。

5. 持續推動資安治理成熟度

持續精進 IT 與 OT 資安治理成熟度機制與評估問項，協助推動

IT 與 OT 資安治理成熟度評估作業，包含辦理 IT 與 OT 資安治理成熟度評估機制說明會、提供評估問項諮詢服務等，以持續提升公務機關與關鍵基礎設施提供者之 IT 與 OT 資安治理成熟度等級。

研析各國關鍵基礎設施領域之工業控制系統資安防護相關文件，做為我國關鍵基礎設施領域工控系統資安防護與相關管理作為之參考。

6. 推動國家層級資安風險評估機制

蒐集國內外重大資安事件與關鍵基礎設施領域資安威脅趨勢，持續推動各關鍵基礎設施領域導入國家層級資安風險評估機制，並偕同關鍵基礎設施領域主管機關與提供者完成領域國家層級資安風險評估作業，掌握我國關鍵基礎設施之資安威脅與風險。

7. 擴大參與國際資安合作交流

加入國際主要資安組織 FIRST、APCERT 及 APEC TEL 等，並擔任督導委員或工作組召集人，拓展我國國際影響力。建立與他國之雙邊或多邊合作，參與國際或區域性資安演練，強化跨國資安聯防。

與國外頂尖技術或學術研究機構進行專案合作，強化我國資安技術與研發、制定新興資安策略與規範等相關能量。

8. 綜整研析資安情勢

為提升國家資通安全科技能力、推動資通安全科技研發及應用為觀點，觀察國內外資安威脅趨勢，發行資通安全技術年報，回顧全球與國內政府機關發生之資安事件，分析其衝擊與後果，說明我國因應防護作為與整體防護綜效，做為強化資安防護、投入研發資源及掌握我國資安現況之參考。

9. 辦理跨國攻防演練

運用虛擬化平台建置模擬醫療領域關鍵基礎設施環境，並以虛

實串接方式結合 IT 與 OT，打造出仿真且完整之醫療領域工控模擬場域，做為紅藍隊對抗場域。邀請我國關鍵基礎設施領域之資安(訊)人員擔任藍隊，並邀請國內外資安團隊擔任紅隊，以即時紅藍隊對抗方式，辦理跨國攻防演練活動。

(三) 政府網路資安縱深防護

1. 攻擊研析與偵測防護

(1) 實施網路攻防演練

針對政府機關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，同時搭配社交工程演練及分散式阻斷服務攻擊，主動發掘潛藏於機關為民服務資通系統弱點，強化資通系統資安防護，並維運社交工程演練系統，提供機關自行測試機關人員資安意識。

(2) 規劃及建置關鍵基礎設施攻防演練場域

參考關鍵基礎設施提供者之資通系統(Information Technology, IT)與工業控制系統(Operation Technology, OT)環境、網路區域劃分方式、軟硬體版本及運作模式，進行關鍵基礎設施攻防演練場域建置。

(3) 綜整分析駭侵特徵與強化偵測防護機制

透過分析事件處理、中繼站調研、資安健診及外部情資等各項來源之惡意程式樣本，萃取網路攻擊流量特徵，製作並部署偵測規則於政府領域防護偵測機制，同時配合各項來源情資進行關聯，進一步分類歸納駭侵活動之特徵，針對發動攻擊之族群進行辨識與追蹤，強化我國網路安全防護能量。

(4) 提供專業資安通報與諮詢服務

協助通報機關處理資安事件，於限定時間內完成復原或損害

管制，並提供損害管制建議。透過通報應變網站，掌握公務機關與特定非公務機關資安防護情形。

(5) 協助資安事件處理與鑑識分析

依據機關資安事件通報所需技術支援，或因應特定單位檢測與中繼站調研需求成立協處專案，提供遠端分析與現場鑑識之技術協助，評估影響範圍，分析包含流量、檔案系統、記憶體及日誌紀錄等取得事證，查找事件根因並提出改善建議，俾利儘速進行應變，降低事件影響與衝擊。

2. 政府領域聯防監控及資安防禦向上集中

(1) 綜整分析端點偵測資料，提升資安防護

協助政府機關與其 SOC 廠商針對不同 EDR 產品進行事件告警資料回傳與格式介接測試，彙整 A、B 級公務機關之端點偵測事件資料，並進行統計與關聯分析，以利掌握駭客攻擊手法與趨勢變化。

(2) 實施重大資安警戒專案

協助於國家重要慶典及政府機關執行特定業務期間成立資安警戒專案，提供 24 小時資安事件即時監控服務、識別可能資安威脅即時預警應變、維持相關服務運作正常，確保資安事件通報應處流程管道順暢。各專案結束後說明該期間執行成果，就各機關通報事件受駭情況與原因進行分析及精進。

(3) 協助防護重點機關資安

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 7x24 資安警示作業，透過資安警示系統收容重點機關網路產生之各類型資安事件紀錄，藉由關聯規則自動化偵測機制開立資安工單後，透過人工確認與

判斷資安事件威脅類型，即時進行資安事件追蹤與警訊發布作業。

(4) 資安防禦向上集中

- 建立誘捕偵測資安防護機制

  維運政府機關誘捕偵測資安防護機制，定期收容部署點之誘捕資料，偵測針對我國之駭侵活動，即早預警國內之攻擊威脅，以提升政府機關威脅偵測能量。

- 自動化黑名單阻擋作業

  維運自動化黑名單部署服務系統，持續推動政府機關導入黑名單自動化部署，提供機關自動化讀取黑名單情資，減少機關手動部署作業，以利提升阻擋攻擊之效率，強化資安聯防。

- 偵測防護政府機關惡意電郵

  透過政府重點機關之惡意電郵情蒐機制，偵測惡意電子郵件威脅與萃取中繼站資訊，分析惡意電子郵件所造成之影響，並至機關進行現場服務與設備更新。

3. 協助推動零信任網路資安防護

持續蒐整國內外零信任網路技術與政策發展狀況，基於已發布之功能符合性驗證檢核表，精進零信任機制核心基準導入指引，以及研擬零信任架構資安防護成熟度自評表，供機關參考，以利評估現況、規劃導入零信任之解決方案及促進提升零信任架構整備度。另研析網路微切分之實施方式，供後續擴充零信任架構之應用情境，強化政府機關之主動防禦能量。

4. 綜整及分享國內外資安情資

維運國家資安資訊分享與分析中心(N-ISAC)，持續收容與整合

國內外資安情資，精進情資收容、整合、分析及分享之能量，強化N-ISAC 會員間互信關係，促進公私協同合作，以提升國家資通安全整體防護與應變能力。

持續進行國際資安情資交流與國際資安事件通報，落實情資分享等交流工作，與各國資安組織維持暢通之聯繫管道。

5. 維運與精進資通安全弱點通報機制

積極推動資通安全弱點通報機制，協助政府機關與關鍵基礎設施提供者，導入並持續維運資通安全弱點通報機制(VANS)，研析擴大推動納入核心網通設備之作法，並定期追蹤資通安全責任等級 C 級以上機關 VANS 執行情形。

持續維運與精進資通安全弱點通報系統，提供系統帳號與 API 介接申請、開通及提供技術諮詢服務，並推動 CPE 轉換正確率測試機制，輔導共契廠商提升 CPE 轉換正確比率；配合資安服務團，提供實地輔導，持續蒐整相關問題與建議，納入後續精進之參考。

(四) 技術基準研究

1. 研究發展政府組態基準

研究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，提供政府機關部署之參考。製作安全組態基準實作文件與數位影片，透過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，提升政府資安韌性。

2. 推動技術移轉與創新育成

透過廣泛推廣研究成果，推動資安技術發展，提升國內企業競爭實力，以創造技術創新與移轉之雙贏局面，同時奠定本院資安研發領域領導地位，進一步促進資安產業蓬勃發展，為國家科技領域進步做出卓越貢獻。

3. 研析重大資安弱點

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，針對重大弱點進行研析與評估可能造成之影響，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，以提升弱點修補速度。

針對掌握弱點情資，評估是否為我國資通訊環境常用系統或應用程式之潛在重大弱點，蒐集相關檢測工具或攻擊程式，架設模擬環境與測試弱點利用可行性，產出重大弱點研析與實作報告，並公布於官網，協助公私部門進行弱點檢測、評估及修補作業，強化資安防護能量。

(五) 強化委外風險管理

1. 辦理資安服務團

配合資安署 114 年資通安全防護輔導服務作業計畫，辦理 10 場資安服務團，輔導機關落實資通安全管理法法遵要求，與協助機關推動精進策略面、管理面及技術面相關安全防護措施，並提供實務專業建議做法。

資安服務團原則分為「輔導訓練」與「實地輔導」2 個階段執行，並按受輔導機關類型針對至少 10 項議題(如資安治理成熟度、資訊委外安全管理及網路安全管理等)規劃及辦理防護輔導服務。

2. 協助資安服務共同供應契約規範檢視

因應資安服務納入共同供應契約，為協助政府機關以合理價格取得合規之資安服務，檢視現行至少 5 份之資安服務共契採購規範內容。

3. 精進資安服務廠商評鑑機制

辦理 SOC 服務、資安健診、弱點掃描、滲透測試及社交工程演練等 5 類資安服務廠商評鑑作業，並辦理至少 1 場資安服務廠商說明會，洽請 3 家公協會協助邀請相關資安服務廠商與會及參與評

鑑。

針對廠商評鑑執行情形，蒐整各機關與廠商之回饋意見，據以精進未來評鑑機制與評分方式，提出相關精進建議。

(六) 強化台灣電腦網路危機處理暨協調中心(TWCERT/CC)

1. 建立及推動資安漏洞通報與揭露機制

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)身分審核並發布 CVE 編號，維運台灣漏洞揭露(Taiwan Vulnerability Note, TVN)平台，受理與審核針對我國產品存在資安漏洞疑慮之申請，並協助溝通、修補及發布 CVE 編號與相關漏洞資訊，強化資安漏洞處理防護系統，提升我國產品安全性。

2. 協助企業通報資安事件及應處

為使中小企業發生資安事件時，可獲得專業應變處置建議，設置企業資安事件通報窗口，包含網站與電子郵件等通報管道。接獲企業通報後，由專人了解事件發生概況，提供資安事件處置建議，如涉及 APT 攻擊活動，視企業需求提供到府技術協助。此外，透過企業提供攻擊情資，通報攻擊來源組織單位，以達到聯防協處之成效。

接收各領域中央目的事業主管機關針對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作業，檢視調查報告，確認強化改善作為之有效性。

3. 發行資安情資電子報

不定期彙整國內外資安「新聞訊息」、「資安活動」、「資安小知識」、「資訊安全宣導」及「漏洞資訊」等資料，並於台灣電腦網路危機處理暨協調中心(TWCERT/CC)官網發布，以供民眾瀏覽資安訊息，提升資安意識，同時彙整每月發布之資安資訊，以電子

報方式主動發布予訂閱民眾，促使民眾可獲得當月重要資安訊息。

4. 參與國際資安組織活動

參與 3 場國際大型資安研討會議，如 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固定舉辦之活動及 RSA 會議，做為我國對外之主要窗口。

5. 提供惡意檔案檢測服務

提供惡意檔案檢測服務，持續進行系統功能更新與維運，藉由蒐集各單位上傳之惡意檔案，建立台灣惡意檔案威脅之樣態，掌握樣本類型分布變化。萃取中高風險惡意檔案威脅情資，進行資安聯防。

6. 掌握上市櫃公司重大資安事件

金融監督管理委員會於「重大訊息發布應注意事項參考問答集」，明確要求上市櫃公司發生資安事件，應發布重大訊息。本院透過公開資訊觀測站(https://mops.twse.com.tw/mops/web/index)每月蒐整上市櫃公司資安事件概況，掌握民間企業遭攻擊情形與事件原因，可做為企業資安宣導題材來源，以強化我國企業網路安全，提升資安防護能量。

7. 強化公私聯防機制

接獲公務機關或企業通報因供應商產品 Zero-Day 漏洞攻擊成功或產品漏洞審核等級達 9 以上時，主動與該供應商建立聯繫管道，掌握其服務範圍與影響對象，並了解漏洞修補與更新概況，追蹤修補進度，以確保資安法納管對象不受該漏洞影響。

(七) 協助維運資安管理相關資通訊系統

配合資安署業務需求，維運委託代管之資通系統，進行系統功能開發維運，並進行系統功能模組擴增與強化。以資安法規範之資通系

統防護基準為基礎，持續進行資通系統之安全檢視與強化，包含防護基準安全需求實作方式、定時進行原始碼檢測、弱點掃描、滲透測試及留意漏洞警訊公告，並評估是否需要進行元件更新，以符合防護基準要求。

二、辦理政府韌性系統服務工作執行計畫

協助數位發展部數位政府司(以下簡稱數政司)執行「辦理政府韌性系統服務工作執行計畫」，包含「整體政府資通安全防禦技術暨系統韌任強化計畫」、「規劃協調及推動政府辦公智慧化」及「規劃協調及推動政府便民資通訊系統」等 3 項計畫。

(一) 整體政府資通安全防禦技術暨系統韌任強化計畫

研擬「建構政府安全與韌性環境服務機制」、「充實政府共享數位資源」、「厚植政府資訊系統運作韌性」及「強化政府資訊系統緊急事件應變能量」等 4 大發展策略，以提升政府機關資訊系統持續運作能力，精進資訊系統服務品質，增強資通安全防護量能，協助政府機關善用數位力量輔助解決社會重大事件及政府施政措施。

1. 建構政府安全與韌性環境服務機制

藉由建立服務團隊，推動數位服務設計及數位服務流程再造，協助探詢、建置與整備政府機關資訊系統共用資訊資源，研析資訊系統資安環境，並辦理民生關鍵業務之大型資訊系統或跨機關業務流程整合系統(以下簡稱民生關鍵資訊系統)巡航作業。

主動或依機關申請即時監測民生關鍵資訊系統運作情形，發現系統異常主動通知業務主管機關與資訊系統維護廠商共謀解決方案。協助進行「事件與鑑識分析」查處異常事件，並視異常狀況複雜程度「籌組專家團隊」對症下藥，以協同主責機關快速回復系統運作，持續強化政府安全與韌性環境，並累積資安自主防護能量。

2. 充實政府共享數位資源

透過建構軟體物料清單(Software Bill of Materials, SBOM)、資訊專案文件與開源碼詮釋資料中文化，以及擴充政府設計系統元件，提供一致且便於操作之設計系統元件，予政府機關建構數位系統使用，除提升民眾使用政府資訊系統之數位體驗，避免因人為失誤，導致之系統運作失效風險，強化政府整體資訊系統的韌性能量。

3. 厚植政府資訊系統運作韌性

盤點行政院及其所屬機關涉及民生關鍵資訊系統，調查其基礎背景資料，並擬定年度數位韌性巡航計畫，透過工作坊培養數位韌性領航員。

依據數位發展部核定年度數位韌性巡航計畫及年度領航員名單，由政府安全與韌性環境服務團執行數位韌性健檢作業，協助業務主管機關診斷資訊系統脆弱點。於實地輔導後，彙整輔導報告並提出資訊系統提升方案。

另依受檢機關需要提供技術支援顧問服務，協同業務主管機關及其資訊系統服務廠商共同改善資訊系統脆弱點。透過檢視文件、工具驗證及領航員實地查驗等方式，檢視補強情形，對未改善或改善情形不如預期者進行技術支援與輔導，納入次年健檢標的。

4. 強化政府資訊系統緊急事件應變能量

主動即時監測民生關鍵資訊系統運作情形，發現資訊系統運作韌性已達到崩潰時，主動通知業務主管機關與資訊系統維護廠商共謀解決方案並提供諮詢服務。當接獲各機關臨時性事件處理與任務性資訊系統之緊急事件時，除應急事件檢查與排除外，並提供應急事件之後續改善建議。

定期觀測國際數位政府治理與推進策略，並透過與專家或相關組織之交流、討論，針對數位政府之治理與推進策略提出建議供主管機關參考。

(二) 規劃協調及推動政府辦公智慧化

著重於政府零信任架構推廣與導入，以建立安全可靠的運作環境，且所傳輸的機敏資訊不受到未經授權的存取與攻擊，以確保政府服務韌性。

輔導 A 級機關導入設備鑑別技術，提供機關技術諮詢管道與相關導入文件參考，協助政府機關藉由零信任環境架構，強化政府服務韌性運作。透過各機關訪談與實地輔導方式，瞭解機關跨境公有雲樣態，並提供機關關於跨境公有雲於合規與執行面之具體建議。另針對 GSN 網路 AI 模型與政府資訊防偽共通資訊平台分別進行概念驗證，以打造更具安全與可靠之政府服務環境。

(三) 規劃協調及推動政府便民資通訊系統

為確保政府數位服務之安全、可靠及易用，將雲原生系統架構原則與服務導入、APP 無障礙驗證工具之自動化架構、數位服務設計流程指引、AIOps 工具或服務導入及 AI 模型在使用者體驗分析應用之概念驗證等工作，以打造更具彈性、便利與無障礙性之數位服務環境。

三、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

協助數位發展部韌性建設司(以下簡稱韌性司)執行「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」，結合技術、人才及通傳事業夥伴關係，透過公私領域協力合作，強化通傳網路之資安監控、分析、通報及應處，並完備通傳網路關鍵基礎設施監理，創建安全、可靠及具韌性之國家關鍵通傳網路。

(一) 維運管理 NCCSC 平臺

檢視 C-NOC 平臺，視實際需求進行功能調整優化，規劃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。

(二) 協助督導關鍵電信基礎設施設置者落實資通訊設備 CVE 漏洞修補作業

關鍵電信基礎設施設置為維繫國家整體電信網路順暢運作之核心，為確保該等電信基礎網路重要節點之資通訊安全，強化電信網路續運運作韌性，將協助韌性司依電信管理法第 42 條第 7 項規定，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，避免衍生資安事件。

(三) 配合辦理 A 級機關應辦事項

數位發展部為資通安全責任等級 A 級公務機關，適用範圍包含 NCCSC 場域與相關人員，配合數發部資訊處發行之資訊安全管理系統程序/表單，結合既有「NCCSC 場域人員及門禁管制規範」執行資安控制措施，辦理 A 級機關應辦事項之管理面、技術面及人員認知與訓練等項目。

(四) 辦理通傳事業資安攻防演練

針對通傳事業之對外服務系統，以模擬駭客攻擊方式辦理資通系統實兵演練，以評估通傳事業單位之網路攻擊防禦能力，以及提升其偵測與應變能力。

(五) 辦理通傳事業資安教育訓練

藉由辦理通傳事業資安防護教育訓練，提升資安意識，蘊育資安能量，依其業務職掌分為策略面、管理面及技術面等 3 個面向之應備能力，強化資安控管措施，支援資安即國安政策，並孕育通傳領域資安相關人才。

(六) 辦理通傳事業情資分享會議

彙整通傳網路運作平臺與通傳資安監控分析通報平臺情資，辦理通傳事業情資分享會議，深化通傳領域防護能量，提升資安意識，強化資安聯防機制。

(七) 辦理通傳領域關鍵基礎設施提供者資安稽核作業

依資通安全管理法要求，中央目的事業主管機關應稽核所管關鍵基礎設施提供者之資通安全維護計畫實施情形。協助韌性司針對選定之通傳領域關鍵基礎設施提供者辦理資安外部稽核，以持續精進資安防護水準。

四、 AI 網路主動式防禦關鍵技術研究計畫

協助數位發展部數位策略司(以下簡稱策略司)執行「AI 網路主動式防禦關鍵技術研究計畫」，利用 AI 建立威脅情資自主智慧分析技術，進而研發戰情匯流智慧追跡技術，期透過 AI 強大分析能力，以更智慧、自主方式協同處理威脅情資，提高應對未來網路威脅整體效能。同時，強化政府機關在資安防護、監控、預警管理及通報等緊急應變能力，全方位提高我國數位生態防護能力，達成應變韌性政策目標。

(一) 推動資安技術 AI 化

利用 AI 建立威脅情資自主智慧分析技術，進而研發戰情匯流智慧追跡技術，依據其特性主要分為三大技術開發項目「威脅態勢預警」、「攻擊酬載來源鑑別」、「未知漏洞風險識別」及整合型「戰情匯流追跡」技術。

(二) 推動 AI 網路主動防禦研發生態系之友善環境

1. 綜整研析 AI 應用政策及法規治理

考量網路主動防禦之應用情景，研析國際間已聚焦或正在形成之人工智慧相關規範、指引及標準，綜合篩選出對應用 AI 於網路主動防禦最重要或預期有持續影響力之規範原則及其可能之未來演

進，進一步分析於此環境下，產業同步其研發布局、法規遵循或其他規範議題時之可能著力處。

研析政府如何於規範面提供機制或鼓勵市場推出不同機制，降低產業投入 AI 網路主動防禦之資安或相關規範風險，以平衡產業對效能與效率及人工智慧相關規範或其他規範對基本人權、民主秩序等價值之追求。

2. 發展 AI 主動防禦教材

訓練課程將由 AI 與主動式防禦技術出發，研析所需資安知識與技能，講解 AI 於資安防護領域之應用情形，並搭配案例示範，幫助學員建構 AI 主動式防禦技術完整概念。

3. 推動技術移轉

為深化 AI 網路主動防禦技術的有效轉化，規劃舉辦 2 場次 AI 網路主動防禦技術/情報交流會，推動最新 AI 網路主動防禦技術，促進相關領域專業知識的深度交流。

五、資料保護驗測機制推動計畫

協助數位發展部多元創新司(以下簡稱多元司)執行「資料保護驗測機制推動計畫」，契合數位發展部發展目標，並接軌國際趨勢，將以促進隱私強化技術採用自主評估、降低技術應用門檻、建立技術驗測共識、擴展技術應用場域等策略，協助我國隱私強化技術之研發量能培植及推進技術多元場域之落地應用，期實現隱私強化技術促進數據共享與建構信任的效益。

(一) 發展隱私保護前瞻研究

隱私強化技術並無萬靈丹，納入資料隱私保護強度及可用性評估，掌握新興技術之發展，對應資料使用情境選擇適合之技術方法，才能有效降低風險並保有資料隱私。本計畫於 113 年發展差分隱私、

合成資料、聯合學習與同態加密等不同技術之檢測方法，於 114 年將持續推進技術研究量能，並持續辦理技術檢測，在知識擴散同時，使檢測方法也更加成熟健全。

(二) 擴展隱私強化技術應用

為持續推廣並深耕隱私強化技術在國內的應用與效益擴散，鼓勵跨界之各機構皆能重視資料隱私保護議題，規劃盤點隱私強化技術可能應用場域，主動探詢、媒合或以公開說明會等方式進行技術推廣，並參與相關競賽，以挖掘更多潛在應用新場域，透過與多元場域協作主題式概念性驗證，加速形塑國內隱私強化技術應用案例，促進各界了解隱私強化技術之效益。

六、NICS 台灣資安計畫

為協助中小型與微型企業、非政府組織、社會企業及其他獲取資源能力有限組織等民間組織(以下簡稱輔導對象)，增進資安意識及提升資安防護能力，本院研提「臺灣資安基金計畫」(Taiwan Cybersecurity Fund Initiative，以下簡稱 NICS 台灣資安計畫)，向美國谷歌公司(Google)所屬慈善部門－谷歌資助基金會(Google Grantmaking Foundation，簡稱 Google.org)申請計畫贊助基金，以透過教育、服務及實踐方式，共同打造更加安全之資訊環境。

(一) 台灣中小微型企業及非營利組織資安現況研究

規劃對我國中小微型企業及非營利組織之資安現況進行研究，辦理數場專家諮詢會議，以實際了解輔導對象之資安需求與挑戰。

(二) 編製及推廣資安培訓及提升資安意識系列教材

編製輔導對象所需資安輔導與培訓教材，以及全民資安意識推廣所需教材，以利學習如何建立適合其需求之網路與資安措施。

(三) 提供中小企業資安服務

透過培訓種子師資(Train the Trainer)方式，推出資安評估與能力建構行動計畫，成立「資安服務團」協助中小企業、非營利組織推動落實各項資安政策與措施，以敏捷式資安服務機制，立即改善中小企業與資安資源弱勢團體特定資安議題，提供專業資安培訓，以提升整體資安能力。

(四) 開設網路安全實務與社會課程，培訓資安輔導員

與國內大專院校合作，並與美國網路安全診所聯盟(The Consortium of Cybersecurity Clinics, CCC)建立合作管道，提供我國非營利組織與中小微型組織資安諮詢服務。

(五) 擴展提升資安意識系列活動

透過系列推廣與展示活動，促進全民資安意識之提升。

(六) 鏈結公私部門資源協力推動

與公私部門合作，運用既有相關資源，共同促進中小微型營利/非營利組織資安意識及資安防護能力之提升，以及全民資安意識之提升。

參、年度目標

本院 114 年度各補助計畫工作項目年度目標，詳見表 1。

表1　工作項目與年度目標清單

計畫名稱	工作項目	年度目標
政府資通安全防護工作執行計畫	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
	推動公私協同治理	▪研析並提出資通安全管理法之發展建議

計畫名稱	工作項目	年度目標
		▪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 ▪協助推動 A、B 級公務機關之 IT 資安治理成熟度持續提升 ▪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 ▪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 ▪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
	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 ▪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

計畫名稱	工作項目	年度目標
		▪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 ▪完成零信網路導入與研析執行報告 ▪新增收容 2 種國際資安威脅指標，強化情資分享內容 ▪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
	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
	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

計畫名稱	工作項目	年度目標
		約規範 ▪辦理現行 5 類資安服務廠商評鑑作業
	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
	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
辦理政府韌性系統服務工作執行計畫	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 ▪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 ▪盤點民生關鍵資訊系統背景資料 20 項 ▪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

計畫名稱	工作項目	年度目標
		技術輔導與執行改善複審作業
	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 ▪完成 1 個政府資訊防偽共通資訊平台 POC 驗證 ▪輔導 A 級機關導入零信任設備鑑別技術，完成 19 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
	辦理各級政府數位服務應變與公私協力環境規劃、營運與輔導服務	▪完成雲原生系統架構原則與服務導入文件 1 式 ▪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
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	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

計畫名稱	工作項目	年度目標
	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
	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
	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
	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
	辦理通傳情資分享會議	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
AI 網路主動式防禦關鍵技術研究計畫	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
	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

計畫名稱	工作項目	年度目標
		▪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
資料保護驗測機制推動計畫	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
	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
NICS 台灣資安計畫	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
	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)
	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

計畫名稱	工作項目	年度目標
	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
	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
	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

肆、年度經費需求

114 年度政府專案補助收入計 620,005 千元(經常門 540,618 千元，資本門 79,387 千元)，與專案委辦收入計 17,500 千元；重點說明如下，經費需求詳見表 2。

一、人事費用

正式人員 230 人年與合聘人員之實際薪資、獎金、退休金及保險等費用，經費預估 340,076 千元。

二、業務費用

業務費用經費預估 218,042 千元，包含營運管理費用水電、郵電、旅運費、設備/用品耗材、房租、設備租金及稅捐等營運費用 89,305 千元；電腦軟體服務費用及各項雲端服務費用 99,361 千元；勞務委外費用

8,175 千元及其他業務費用 21,201 千元。

三、資本門費用

固定/無形資產建設改良擴充費用經費預估 79,387 千元，為執行業務所需，採購或汰換更新電腦相關設備等預估 59,787 千元，採購/擴充電信相關設備等預估 12,000 千元，以及新增海纜內陸介接站之設施暨服務告警收容及 TWISAC 平台與 VIRUSH CHECK 平台開發等電腦軟體費用預估 7,600 千元。

表2　114 年度經費需求

科目及營運項目	預算	說明
經常門		
人事費	340,076	正式人員 230 人年與合聘人員之實際薪資、獎金、退休金及保險等費用，經費預估 340,076 千元，年平均人事費 1,479 千元 ▪ 估算方法：直接薪資=實際薪資 X(1+非經常性給與之獎金%) ▪ 非經常性給與之獎金：包含不扣薪假與特別休假之薪資費用、非經常性給與之獎金及依法應由雇主負擔之勞工保險費、積欠工資墊償基金提繳費、全民健康保險費、勞工退休及卹償金，計約實際薪資 47%，故年平均實際薪資為 1,004 千元
服務費用	188,707	▪ 水電費：辦公室水電費預計 4,762 千元 ▪ 郵電費：公務信件寄送費、電話及網路費預計 21,370 千元 ▪ 旅運費：包含國外出差 47 人次等出差相關費用及推估國內差旅費用及運費等預計 23,175 千元 ▪ 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 1,933 千元

科目及營運項目	預算	說明
		▪修理保養及保固費：辦公設備與房屋修繕養護費預計 14,245 千元 ▪一般服務費：勞務外包費預計 8,175 千元，包含資料蒐集、課程開發、資安開發建置、學研合作、辦理國際研究會議、委外辦公處之設備維護等各項勞務外包；計時人員酬金及派遣人力等費用預計 5,798 千元 ▪專業服務費：電腦軟體服務費預計 99,361 元，包含系統開發與測試電腦軟體授權費及各項雲端服務費用等；派員參加國內訓練費用及各式講座鐘點費等預計 9,000 千元 ▪其他費用預計 888 千元，包含辦公區域建物火險費、機械設備保險費、活動課程保險費(公共意外責任險)及公關慰勞費等
材料及用品費	3,343	▪使用材料費：為設備運轉、維護所耗用之物料預計 550 千元 ▪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、書報雜誌及其他一般事務費預計 2,793 千元
租金及利息	20,695	▪房租：辦公處所租金費用預計 17,700 千元 ▪地租及水租：活動場地租金費用預計 1,568 千元 ▪機器租金：機器設備、辦公事務影印機及活動硬體等設備租用預計 1,277 千元 ▪什項設備租金預計 150 千元
稅捐與規費	573	▪消費與行為稅：各式契約等憑證貼用之印花稅票預計 217 千元 ▪規費：政府機關各項規費費用預計 356 千元

科目及營運項目	預算	說明
會費、捐助、補助、分攤、救助(濟)與交流活動費	3,376	▪ 分攤：分擔辦公處所大樓管理費用預計 2,710 千元 ▪ 參加國內外組織會費 240 千元 ▪ 對國內外團體與個人之捐助及獎勵，以及競賽及交流活動費計 426 千元
其他費用	1,348	辦理各項活動、演練及研討會等之會議費用及其他 1,348 千元
小計	558,118	
資本門(固定/無形資產建設改良擴充費用)		
機械及設備	59,787	執行業務所採購或汰換更新設備，包含為建立 Container 運算平台、高效能儲存、高頻寬光纖網路、移動式 AI 分析、GPU 運算主機、網路交換器、光纖儲存設備、機架型伺服器、備援設備等資訊電腦設備
交通及運輸設備	12,000	零信任網路導入設備、機房環境監控系統建置設備、無線網路建置設備、Qosmos20 Gbps SW Licence (Perpetual LIC)擴增及流量側錄器等網路設備
電腦軟體	7,600	新增海纜內陸介接站之設施暨服務告警收容及 TWISAC 平台與 VIRUSH CHECK 平台開發
小計	79,387	
合計	637,505	