國家資通安全研究院

113年度業務計畫

中華民國112年8月

數位發展部112年8月25日數位策略字第1127001529號函備查

112年7月11日第一屆第四次董監事聯席會議通過

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

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。

依蔡總統「資安即國安」政策及行政院核定之「國家資通安全發展方案(110 年至 113 年)」，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)如下：

(一) 安全(Security)：為建構國家全方位資安防護網，透過情資整合分析、跨域聯防及事件通報協處等方式強化。

(二) 技術(Technology)：透過與產學研各界共同合作研發，期帶動國家資安關鍵技術發展。

(三) 主動(proActiveness)：持續觀測國內外資安情勢發展，擔任國家資安研發幕僚。

(四) 韌性(Resilience)：提供政府機關資安服務，強化機關資安韌性，成為國家資安技術服務標竿。

(五) 信賴(Trust)：強化人才培力能量，培育國家頂尖資安人才與資安防護團隊。

三、推動策略

依「資安即國安」政策，資通安全已提升至國家安全層級，本院以3大目標為依歸，專注國家整體資安防護，面對日益嚴峻之資安威脅與日漸增長之駭侵趨勢。本院為實踐安全(Security)、技術(Technology)、主動(proActiveness)、韌性(Resilience)及信賴(Trust)等5大核心價值，採下列5項推動策略：

(一) 建構資安防護聯網，強化資安預警能量。

(二) 研發資安前瞻技術，帶動自主創研能量。

(三) 觀測各國資安情勢，深化國際合作交流。

(四) 推動公私協同治理，提升關鍵設施韌性。

(五) 培育資安實戰人才，推廣全民資安意識。

本院以願景、3大目標及5項推動策略，建構發展藍圖(詳見圖1)，以執行各項資通安全任務，包含事前、事中、事後各項資安技術服務，更針對資安前瞻技術進行研究，並持續培育高階實戰人才。

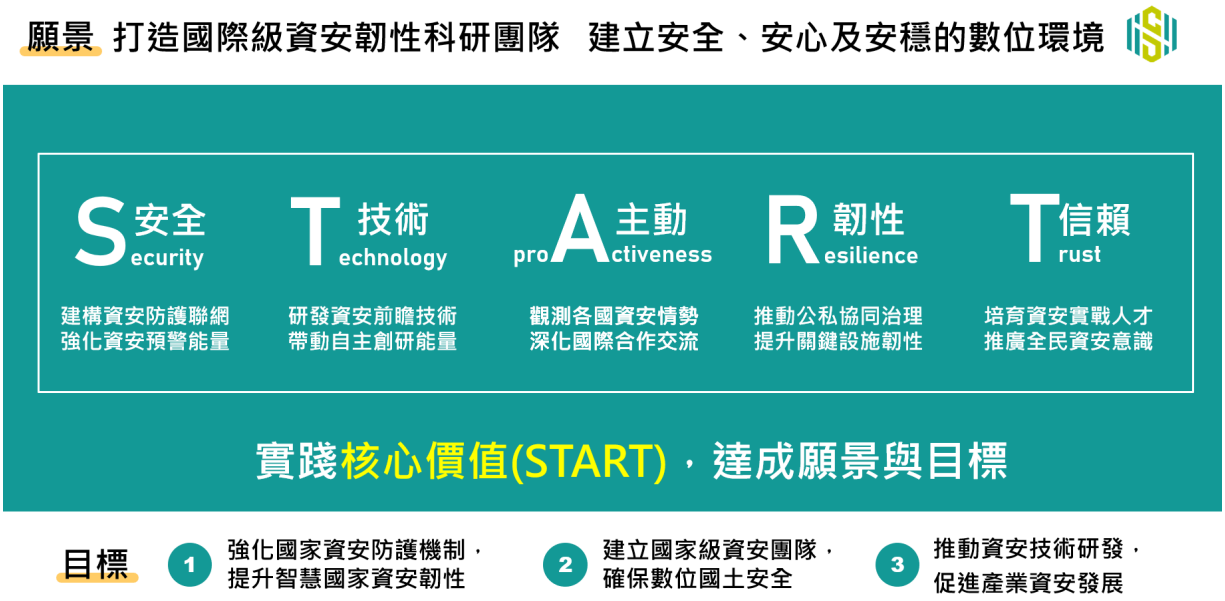

圖1　國家資通安全研究院發展藍圖

貳、年度工作計畫

依據本院業務範圍與 5 項推動策略，承接數位發展部規劃、協調及推動資通安全相關作業，以及「臺灣資安卓越深耕－資安卓越中心計畫」、「整體政府資通安全防禦技術暨系統韌性強化計畫」、「完備通傳領域關鍵基礎設施監督管理計畫」等政府(專案)補助計畫。

本院 113 年度業務計畫依資安院業務範圍並參照政府(專案)補助計畫之架構擬定，期能提升資安應變能力與資安防禦能量，並打造系統之安全性與韌性，協助政府加速建構完善資安環境，促進政府數位系統安全與整備韌性環境，落實公私部門資安管理，帶動整體資安產業向上發展。本院 113 年度業務計畫工作重點說明如下，政府(專案)補助計畫工作項目與推動策略關聯詳見圖 2。

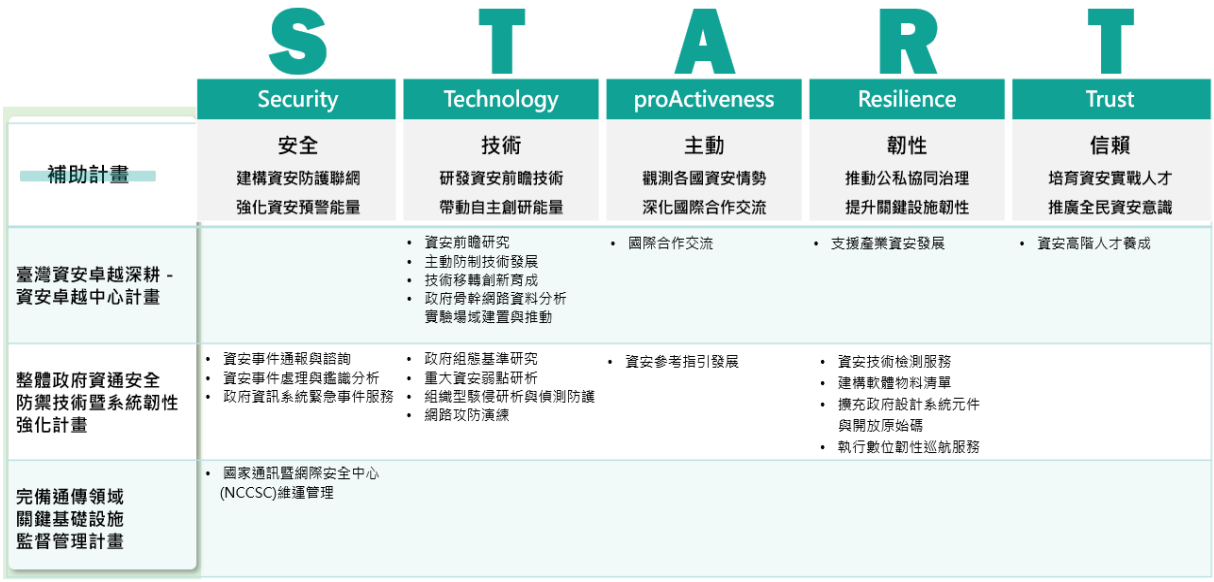

圖2　政府(專案)補助計畫工作項目與推動策略之關聯

一、臺灣資安卓越深耕－資安卓越中心計畫

研析資安前瞻技術暨培訓頂尖資安人才，厚植我國頂尖實戰人才培訓及資安前瞻研究能量，工作項目包含「資安前瞻研究」、「主動防制技術發展」、「技術移轉創新育成」、「政府骨幹網路資料分析實驗場域建置與推動」、「國際合作交流」、「支援產業資安發展」及「資安高階人才養成」等 7 項。

(一) 資安前瞻研究

了解國際資通安全前瞻技術發展，研擬技術研究方向，推動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，包含技術面與政策面等議題，以因應新興科技發展衍生之資安威脅。113 年預計針對分散式通訊技術、後量子加密技術及應用、網路通訊分析模型及情資加值技術等前瞻技術進行研究，發表 9 篇相關論文或技術報告。

(二) 主動防制技術發展

維運主動式防禦應用平台，擴增控制程式支援度，增加可控制對

象之多樣性，完備主動式防禦應用平台功能，以提升主動式防禦應用平台使用場景。

持續擴充系統功能與整合驗證已發展之攻擊情境，驗證駭客攻擊手法與流程，用以剖析新興駭客攻擊手法，協助政府機關因應攻擊威脅與強化資安防護。

(三) 技術移轉創新育成

針對國家需求，盤點本院自行研發及產學研合作之成果，挑選出具發展潛力與市場價值項目，以技術驗證與移轉方式，協助政府機關、關鍵基礎設施提供者，提升其資安技術與管理能力，使研發技術落地運用，推動資安技術應用擴散。

(四) 政府骨幹網路資料分析實驗場域建置與推動

模擬政府網際服務網(Government Service Network, GSN)常見網路服務，建構資料分析試驗環境，供產學合作單位發展網路威脅分析與巨量資料處理架構，促進產學合作。同時擴充現有場域設備，提升場域資料處理容量，增加 Meta data 資料開放量。

(五) 國際合作交流

參與 FIRST、APCERT 及 APEC TEL 等國際資安組織，擔任督導委員會成員與工作組召集人，建立與他國之雙邊或多邊合作關係，參與國際或區域性資安演練，強化跨國資安聯防。

參與國際大型資安研討會，分享國內資安威脅與趨勢，增加台灣國際能見度，維繫國際社群關係。與國外頂尖學術研究機構進行專案合作，建立及提升我國資安技術與研發、制定新興科技政策與規範等相關能量。

(六) 支援產業資安發展

以實務與產學鏈結為導向之創新培育模式，結合國內大學校院及法人資安教學能量，建立以需求為導向之資安人才培訓能量，孕育優質資安人才，提供我國各產業所用。

(七) 資安高階人才養成

1. 實習場域建置

除現有政府機關資安職能課程外，擴大進階訓練，設置資安人培實習場域，強化工控領域訓練，涵蓋工業控制系統(Industrial Control System, ICS)與物聯網(Internet of Things, IoT)。

維運藍隊攻防演練環境，並擴充相關測驗題型等，以協助受試者掌握相關技能，並應用於日常維運工作。該平台可用於資安人員訓練、評核、測驗，協助政府、產業培養具備資安管理與技術之人才。

2. 頂尖實戰人才養成

持續開發藍隊基礎訓練平台題庫，提供學習與演練管道，加強紅藍隊頂尖人才訓練及養成。

招收企業、法人及政府機構之資安資深人員，配合我國資安政策方向及新興資安議題，針對資安專責人員開設進階課程。除課程講授外，每期安排在最後進行防禦平台實戰演練，驗證學習成效。協助企業、法人、政府機構培訓，因應新興資安議題，掌握關鍵資安技術，強化資安防護能量。

3. 開發自主實戰訓練教材

依據規劃之年度重點資安職能工作角色所需之任務、知識、技術及能力，逐步開發資安實務課程，如滲透測試工程師、數位鑑識調查員、資安威脅情資分析師等，議題涵蓋網頁安全(Web Security)、行動裝置安全(Mobile Security)、雲端安全(Cloud

Security)、Linux 系統安全、逆向工程(Reverse Engineering)解析、監視控制與資料擷取系統安全(SCADA Security)及數位鑑識(Digital Forensic)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，並以自主開發國際化培訓教材為長期發展目標。

4. 培訓國家資安戰隊

負責協助實戰型頂尖資安人才養成，擇優挑選產官學軍之人才進行培訓，完訓後獲得較優渥之薪酬及就業機會，並做為國家緊急動員人力之後盾。

招收具資安專長之特定對象，與國內資安社群合作，辦理資安專業課程訓練，代表國家參與各種資安競賽，提升我國於資安領域之國際能見度。強化選手專業技能，投入資安產業或成為資安新創人才。協助辦理我國資安優秀選手之增能活動，以及協助其參與國際競賽。

二、整體政府資通安全防禦技術暨系統韌性強化計畫

促進政府數位系統安全與整備韌性環境，工作項目包含「資安事件通報與諮詢」、「資安事件處理與鑑識分析」、「政府資訊系統緊急事件服務」、「政府組態基準研究」、「重大資安弱點研析」、「組織型駭侵研析與偵測防護」、「網路攻防演練」、「資安參考指引發展」、「資安技術檢測服務」、「建構軟體物料清單」、「擴充政府設計系統元件與開放原始碼」及「執行數位韌性巡航服務」等 12 項。

(一) 資安事件通報與諮詢

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，並提供資安防護建議。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。

(二) 資安事件處理與鑑識分析

依據機關資安事件通報所需之技術支援，或因應特定單位檢測與中繼站調研需求成立專案，提供遠端分析與現場鑑識之技術協助。

針對重大資安事件應處，協助特定非公務機關(公營事業、財團法人及關鍵基礎設施提供者)現場鑑識分析，提升處理時效性與完整性。

(三) 政府資訊系統緊急事件服務

主動即時監測民生關鍵資訊系統運作情形，發生資訊系統運作異常影響民眾個人權益或生活便利性時，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。

(四) 政府組態基準研究

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。

(五) 重大資安弱點研析

蒐集國內外資安弱點情資，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。

針對掌握之上述弱點情資，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，架設模擬環境與進行弱點利用可行性測試，產出重大弱點研析與實作報告，並公布於本院官網，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。

(六) 組織型駭侵研析與偵測防護

分析透過資安事件處理、中繼站調研、資安健診及外部情資等各項來源所蒐集之特定組織型駭侵相關樣本，萃取網路攻擊威脅情資特徵，製作並部署偵測規則於政府骨幹偵測機制，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，並針對特定組織型駭侵族群進行辨識與追蹤，強化政府機關網路防護能量。

(七) 網路攻防演練

針對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，並測試機關人員資安意識，辦理相關演練會議，針對演練執行結果，研討未來精進方向。

(八) 資安參考指引發展

因應國際資安威脅趨勢與新興科技發展等因素，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，並依藍圖規劃時程編撰或修訂資安相關參考指引，且協助資安署持續推動資通安全管理法。

(九) 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。

辦理技術檢測教育訓練，說明技術檢測執行方式與注意事項，藉由實作練習使學員具備執行檢測之能力。

(十) 建構軟體物料清單

持續蒐集與整理政府資訊系統可利用之開源軟體，並建立軟體物

料清單(Software Bill of Materials, SBOM)記錄構成軟體之元件與關聯表，以具可讀性之 SBOM 報告格式呈現，協助政府機關資訊系統使用具完整性與可追溯來源之開源軟體。

(十一) 擴充政府設計系統元件與開放原始碼

持續蒐整設計系統元件、資訊專案文件與開放原始碼詮釋資料，擴大政府機關共享資源，以協助政府機關精進資訊系統之易用性、高可用性、可維護性及安全性，同時便利其引用相關開放原始碼、軟體或服務之參考資料，強化政府機關資訊系統之服務品質。

(十二) 執行數位韌性巡航服務

持續擴大政府安全與韌性環境服務團隊量能，培訓數位韌性領航員，並透過數位韌性巡航，協助政府機關提升資訊系統之易用性、高可用性、可維護性及安全性，使政府機關資訊系統在面對艱困環境下仍能持續提供服務。

三、完備通傳領域關鍵基礎設施監督管理計畫

工作項目為「國家通訊暨網際安全中心(NCCSC)維運管理」。

(一) 國家通訊暨網際安全中心(NCCSC)維運管理

維運管理國家通訊暨網際安全中心(NCCSC)，優化軟硬體設備及場域資安管理與運作，完備通傳網路之資安監控、分析、通報及應處，深化通傳領域資安防護能量，藉由辦理資安教育訓練、攻防演練，提升通傳事業資安威脅防禦意識，強化資安聯防機制。

參、年度目標

本院 113 年度業務各工作項目年度目標，詳見表 1。

表1　工作項目年度指標

推動策略	工作項目	年度目標
1. 建構資安防護聯網，強化資安預警能量	資安事件通報與諮詢	執行公務機關與特定非公務機關資安事件通報與諮詢作業
	資安事件處理與鑑識分析	依需求執行事件處理，提供遠端分析與現場鑑識服務
	政府資訊系統緊急事件服務	主動監測民生關鍵資訊系統運作效能，發生系統效能異常事件 1 小時內通報業務主管機關與系統維護廠商。接獲業務主管機關申請查處異常事件後 4 小時內抵達現場或 2 小時內以線上(視訊)方式進行處置
	國家通訊暨網際安全中心(NCCSC)維運管理	▪辦理 1 場資安攻防演練 ▪辦理 3 場資安防護教育訓練 ▪辦理 4 場資通安全情資分享會議 ▪辦理 7 家關鍵基礎設施提供者資安稽核作業 ▪優化 NCCSC 平臺功能與效能
2. 研發資安前瞻技術，帶動自主創研能量	資安前瞻研究	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
	主動防制技術發展	擴增主動式防禦應用平台
	技術移轉創新育成	▪研發 4 個資安技術應用系統並完成 PoC ▪導入 3 個資安技術應用系統並完成 PoS ▪推動 3 個單位採用或技轉相關研發成果
	政府骨幹網路資料分析實驗場域建置與推動	建置可模擬機關網路環境與應用系統之實驗場域，並開放 6 個月政府骨幹網路 Meta data 資料量，供產學研究

推動策略	工作項目	年度目標
	政府組態基準研究	▪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
	重大資安弱點研析	關注重大資安弱點與發布警訊，每年至少完成 2 個重大資安弱點研析與實作驗證
	組織型駭侵研析與偵測防護	分析駭侵樣本，萃取威脅特徵，製作並部署偵測規則，每年產出 2 項偵測規則
	網路攻防演練	▪執行演練作業，蒐整機關為民服務資通系統弱點樣態，提供各界參考 ▪協助資通安全署遴選機關執行專案網路攻防演練
3. 觀測各國資安情勢，深化國際合作交流	國際合作交流	對接國外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
	資安參考指引發展	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
4. 推動公私協同治理，提升關鍵設施韌性	支援產業資安發展	辦理 1 場技術交流活動，與各界分享國際相關技術發展資訊
	資安技術檢測服務	▪提供 5 個政府機關或關鍵基礎設施資安技術檢測服務 ▪辦理 2 場技術檢測教育訓練
	建構軟體物料清單	整備(新增或更新)30 項軟體模組物件
	擴充政府設計系統元件與開放原始碼	▪調校(蒐集與整理)政府系統設計元件 10 案 ▪完成資訊專案文件與開放原始碼詮釋資料中文化 5 案

推動策略	工作項目	年度目標
	執行數位韌性巡航服務	▪至少完成 3 項民生關鍵資訊系統及 20 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 ▪盤點民生關鍵資訊系統背景資料 13 項 ▪至少辦理 1 場次訓練課程 ▪至少維持 112 年招募或委託技術人員 38 人，專職辦理政府安全與韌性環境服務任務與工作內容
5. 培育資安實戰人才，推廣全民資安意識	資安高階人才養成	▪培訓國內產業與政府所需之資安人才 125 人 ▪持續建置工控場域累積達 4 個，開發 1 套工控場域實戰教材，培訓高階學員達 30 人 ▪開發建置藍隊基礎訓練平台題目至少 30 題 ▪辦理跨國藍隊攻防演練競賽至少 1 場次 ▪招收國際學生 20 人 ▪辦理增能系列活動至少 3 場次，並參與國際資安競賽至少 1 場次

肆、年度經費需求

本院 112 年成立，依營運方針，成立初期以政府補助預算收入為主，暫未辦理財務自籌之業務項目。113 年度政府專案補助預算收入計 712,910 千元(經常門 631,970 千元、資本門 80,940 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 220 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 336,543 千元。

二、業務費用

業務費用經費預估 295,427 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 100,849 千元；電腦軟體服務費用及各項雲端服務費用 67,063 千元；前瞻技術與產學合作開發費用 50,000 千元；勞務委外費用 28,187 千元及其他業務費用 49,328 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 80,940 千元，為執行業務所需，採購或汰換更新設備相關費用預估 62,172 千元，採購/汰換辦公事務設備等預估 800 千元，新增辦公處裝潢費用 15,000 千元，以及 AlgoSec 防火牆政策分析工具、文書編輯軟體及系統擴充等電腦軟體費用 2,968 千元。

表2　113 年度經費需求

金額單位：千元

科目及營運項目	預算	說明
經常門		
人事費	336,543	正式人員 220 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 336,543 千元，年平均人事費 153 萬 ▪ 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、

金額單位：千元

科目及營運項目	預算	說明
		全民健康保險費、勞工退休及卹償金，計約實際薪資 45%，故年平均實際薪資為 105.5 萬
服務費用	243,603	▪水電費：辦公室水電費預計 6,036 千元 ▪郵電費：公務信件寄送費、電話及網路費預計 18,397 千元 ▪旅運費：包含國外出差 96 人次等出差相關費用及推估國內差旅費用及運費等預計 26,941 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 2,224 千元 ▪修理保養及保固費：辦公設備與房屋修繕養護費預計 13,214 千元 ▪一般服務費：勞務外包費預計 28,187 千元，包含巨量資料蒐集、課程開發、DDoS 演練平台系統更新、資安系列競賽、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 12,498 千元 ▪專業服務費：電腦軟體服務費預計 67,063 千元，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；前瞻技術與產學合作開發費用預計 50,000 千元；派員參加國內訓練費用及各式講座鐘點費等預計 18,399 千元 ▪其他費用預計 644 千元，包含辦公區域建物火險費、機械設備保險費、活

金額單位：千元

科目及營運項目	預算	說明
		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	4,735	▪使用材料費：為設備運轉、維護所耗用之物料預計 1,318 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 3,417 千元
租金及利息	34,094	▪房租：辦公處所租金費用預計 18,276 千元 ▪地租及水租：活動場地租金費用預計 5,946 千元 ▪機器租金：機器設備、電信機櫃租用、辦公事務影印機及活動硬體等設備租用預計 9,274 千元 ▪交通及運輸設備租金預計 300 千元 ▪什項設備租金預計 298 千元
稅捐與規費	1,050	▪消費與行為稅：各式契約等憑證貼用之印花稅票預計 450 千元 ▪規費：政府機關各項規費費用預計 600 千元
會費、捐助、補助、分攤、救助(濟)與交流活動費	9,642	▪分攤：分擔辦公處所大樓管理費用預計 2,328 千元 ▪參加國內外組織會費 446 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 6,868 千元

金額單位：千元

科目及營運項目	預算	說明
其他費用	2,303	辦理各項活動、演練及研討會等之會議費用及其他 2,303 千元
小計	631,970	
資本門(固定/無形資產建設改良擴充費用)		
機械及設備	62,172	執行業務所採購或汰換更新設備，包含為建立資安演練平台、政府場域開放資料實驗平台、核心光纖網路交換器、光纖儲存設備、虛擬平台叢集伺服器、執行資安技術檢測使用、弱點研究、軟體物料清單研析等資訊電腦設備
什項設備	800	沙崙院區機房 UPS 電池箱汰換及採購辦公事務設備等費用
租賃權益改良	15,000	新增辦公處裝潢費用
電腦軟體	2,968	AlgoSec 防火牆政策分析工具、文書編輯軟體及系統擴充等費用
小計	80,940	
合計	712,910	