國家資通安全研究院

112年度業務計畫

中華民國112年2月

數位發展部112年2月20日數位策略字第11270002681號函備查

112年1月17日第一屆第二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，具體推動重點如下：

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

(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。

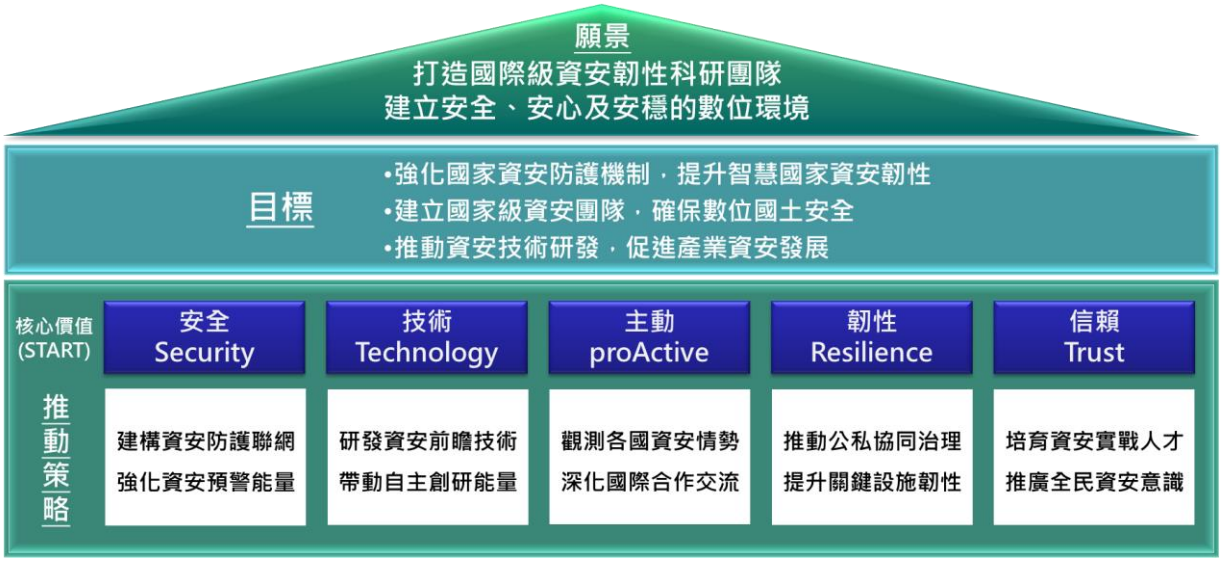
(三) 主動(proActive)：持續觀測國內外資安情勢發展，擔任國家資安研發幕僚。

(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

本院以願景、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。



資料來源：本院整理

圖1　國家資通安全研究院發展藍圖

依「資安即國安」政策，資通安全已提升至國家安全層級，本院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，本院以 3 項目標為依歸，採下列 5 項推動策略實踐 5 大核心價值。

(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。

依本院業務範圍與 5 項推動策略，擬訂 11 項具體作法如下：

(一) 推動資安防護機制，強化國家整體資通安全。

(二) 執行重大事件應變處置，即時阻斷駭客攻擊，強化損害管控。

(三) 精進並推動資安防護技術，支援敏感性政府機關資安防護。

(四) 研發資通安全科技，厚實核心技術自主能量。

(五) 推動產學合作，進行技術整合與移轉，提升產業資安技術水準。

(六) 研析各國資安趨勢，奠定資安智庫地位，提供優質資安建議。

(七) 積極參與國際活動，擴展國際合作交流，提升我國資安能見度。

(八) 運用資安技術，推動資安技術應用，提升政府資安韌性。

(九) 進行資安情資分享與技術交流，支援產業資安重大發展。

(十) 推動資安職能訓練，培育資安實戰人才，打造資安韌性團隊。

(十一) 推廣全民資安認知，提升國人資安意識。

貳、年度工作計畫

依據上述 11 項具體作法，擬訂業務計畫，期能完善資安聯防體系，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。各項具體推動作法之 112 年度業務計畫工作重點說明如下。

一、推動資安防護機制

掌握我國資安威脅情資，進行資安情資整合應用，強化黑名單自動化部署、政府領域資安情資掌握、惡意電子郵件威脅資訊蒐整，產製自主威脅聯防情資，掌握組織型駭客手法與影響範圍，協助機關阻擋惡意郵件攻擊，建構完整防禦陣線，以強化我國資安聯防體系。業務架構包含「1.1 政府領域聯防監控」、「1.2 資安情資分享」、「1.3 資通安全弱點通報」、「1.4 零信任網路資安防護」、「1.5 端點偵測資安防護」、「1.6 政府領域威脅戰情資訊掌握」、「1.7 誘捕偵測資安防護」、「1.8 黑名單自動化阻擋」、「1.9 惡意電郵偵測防護」及「1.10 關鍵基礎設施資安防護技術支援」等 10 項工作項目。

(一) 政府領域聯防監控

訂定政府領域聯防監控情資格式，導入 STIX 2.1 標準格式，擴充收容端點偵測防護情資，萃取與產製聯防監控情資，強化資安聯防能量。

(二) 資安情資分享

強化國際情蒐合作，增加全球共通性資安情資，成為國內主要情資整合與分享平臺，並持續拓展國家層級資訊分享與分析中心(National Information Sharing and Analysis Center,N-ISAC)會員，規劃開放情資分享，提供學研單位或國際資安組織參考。

(三) 資通安全弱點通報

擴充現有資通安全弱點通報系統(Vulnerability Alert and Notification System, VANS)效能與容量，運用平行處理或負載平衡技術，提升系統執行效率，精進關聯分析方法，提升弱點比對效率，以完備資通安全弱點通報機制，提升機關弱點防護能力。

透過執行實地輔導作業或製作數位課程影片，協助機關導入資安

弱點通報機制，並協助政府機關與關鍵基礎設施提供者導入作業。

(四) 零信任網路資安防護

推動政府機關逐步導入零信任網路，以因應遠距辦公與資源向上集中之資安防護需求，並強化政府機關之主動防禦能量。依零信任網路部署機制之規劃，協助我國資安廠商發展符合政府零信任網路資安防護需求之解決方案。

(五) 端點偵測資安防護

協助機關落實端點偵測與應變機制(EDR)之導入與偵測資料回傳作業，有效強化整體惡意程式之偵蒐，以及攻擊趨勢與目標對象之研判。

(六) 政府領域威脅戰情資訊掌握

掌握政府網路面臨之網路威脅樣態，產製台灣自主網路威脅聯防情資，強化我國資安聯防體系。彙整政府領域資產威脅與網路攻擊情資，提供資安威脅戰情資訊，掌握政府資安威脅與防護情形。

(七) 誘捕偵測資安防護

推動資訊資源向上集中機關導入內網威脅誘捕與偵測防護機制，偵測內網駭侵活動，提升政府機關內網威脅偵測能量，即早預警處理。維運網路威脅誘捕系統，分析網路攻擊威脅並產製偵測指標，提供我國資安聯防與國外合作資安組織處理。

(八) 黑名單自動化阻擋

開發威脅資訊整合系統，自動產出黑名單，並建置可供大量設備存取之自動化黑名單部署服務系統，推動機關導入黑名單自動化部署，以加速黑名單更新頻率，提升攻擊阻擋效率。

(九) 惡意電郵偵測防護

推動資訊資源向上集中機關導入惡意電郵偵測機制，維運惡意電郵情蒐分析系統，偵測惡意電郵威脅與萃取中繼站資訊，強化政府機關惡意電郵防護能量。

(十) 關鍵基礎設施資安防護技術支援

1. 工控領域資安治理成熟度

推動工控領域資安治理成熟度評估機制，並協助 A 級關鍵基礎設施提供者完成自評作業。

2. 國家層級資安風險評估

推動關鍵基礎設施領域導入國家層級資安風險評估機制，並擇 6 個 A 或 B 級關鍵基礎設施提供者完成國家層級資安風險評估作業。

二、執行重大事件應變處置

全時監控機敏機關網路，維運政府機關資安通報應變機制，掌握資安事件發生與處理狀況，提升緊急應變處理能量，降低資安事件衝擊，並研析與精進國家重大資安事件應變。業務架構包含「2.1 資安通報與諮詢」、「2.2 資安事件處理與鑑識分析」及「2.3 政府資訊系統緊急事件服務」等 3 項工作項目。

(一) 資安通報與諮詢

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。

(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。

三、支援敏感性政府機關資安防護

擴大追蹤高風險機關資安防護情形，強化組織型駭侵偵測防護，規劃擴充政府骨幹網路流量偵測與分析機制相關硬體效能，升級各重點機關監控設備，提升機關預警之正確性與時效性。業務架構包含「3.1 重點機關資安監控與防護」工作項目。

(一) 重點機關資安監控與防護

於國家重要慶典與政府機關執行特定業務期間，成立資安警戒專案，確保政府機關資安通報管道暢通，並識別可能資安威脅即時預警應變。

重點機關監控設備升級汰換，以利日誌分析類型與關聯規則制訂，強化重點機關資安監控防護。

四、研發資通安全科技

掌握新興技術發展趨勢，進行前瞻研究及資安技術應用，擬定研發策略與設計機制，以形塑國內良好資安技術研發環境。同時利用本院核心技術能量，蒐集政府、學術及民間網路資安威脅情資，建立跨政府機關資安聯防監控機制，研析國內外資安威脅，建立預警機制，並透過公私協同合作進行資安情資分享，降低我國資安風險。業務架構包含「4.1 資安前瞻研究」、「4.2 殭屍網路情蒐研析」、「4.3 政府領域網路威脅研析」、「4.4 社交工程情蒐研析」、「4.5 政府組態基準研究」、「4.6

主動防制技術發展」、「4.7 重大弱點研析」、「4.8 組織型駭侵研析與偵測防護」、「4.9 網路攻防演練」及「4.10 零信任網路產品功能性檢核服務建置」等 10 項工作項目。

(一) 資安前瞻研究

瞭解國際資通安全前瞻技術發展，研擬技術研究方向，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。

1. 多媒體內容原創性鑑別技術之研究

透過多媒體素材鑑識與語意識別技術，進行溯源分析與一致性分析。當輸入一組相關多媒體素材時，可依據素材重疊範圍、修改特徵，識別該素材經過變造部分，以及與其他素材之間的版本演變先後次序。相關成果可移轉及協助網路平台或執法與鑑識機構進行判讀。

2. 隱私權保護技術之研究

透過語意分析與知識圖譜檢索等背景技術，進行網路隱私權防護機制與技術的研究。用於解決使用者因隱私權意識不足，於網路平台揭露過多個人資料，以至於遭受社交工程滲透攻擊，如魚叉式釣魚信。或因私人糾紛導致個人資料被置於公開平台進行公審、網路霸凌等個人權益侵害之行為。相關成果可移轉或協助網路平台或執法與鑑識機構進行判讀。

3. 數位資料外洩溯源追蹤技術之研究

機關、私人企業因業務需求，掌握用戶資料，如生日、地址、信用卡資訊。當遭遇駭侵攻擊後可能於暗網出售個資，再經由媒體報導，除造成個人損害之外，亦對機關的公信力與公司之商譽造成嚴重損害。研究數位資料外洩路徑與分析其特徵，可協助資料持有單位及早發現外洩事件，並將所分析得外洩資料路徑之特徵納入資

安通報、漏洞修補與防詐警示的措施，避免後續衍伸損害擴大。相關成果可移轉及協助公、私部門自我檢測，或執法與鑑識機構進行溯源與判讀。

4. 情資與目擊系統開發

查找存在於內部網路之惡意主機或流量，發掘潛在網路威脅，增進抵禦威脅能力，並提出具體之解決建議，提升國家資安體質。

- 情資分析與自動標記

  透過網路收集情資報告，經自動化分析後產生知識本體(ontology)，並自動標示 MITRE 之戰術(tactics)、技術(techniques)及子技術(sub-techniques)。

- 基於機器學習識別相似之未知惡意流量

  以機器學習方式，開發可識別惡意流量之模型。

- 基於深度學習之主機式多資料源入侵偵測機制

  發展基於多資料源與深度學習之主機式入侵偵測系統。

5. 漏洞挖掘平台開發

- 可驗證之模糊測試

  研究模糊測試之可再現性(reproducibility)，並開發支援可再現性之模糊測試工具。

- 透過動態符號執行挖掘漏洞

  利用動態符號建立擬真執行(concolic execution)軟體技術，開發高效與高準確度漏洞挖掘技術。

- 整合式模糊測試平台

  透過程式資料集、執行環境管理及視覺化，建立整合性平台，

用於學習、研究及評估軟體測試於動態分析之演算法，包含蒐集與管理程式資料集，應用程式介面(API)可供分析，以及視覺化呈現分析結果與過程。

6. 實作與檢定後量子密碼演算法或協定

透過實作與檢定後量子密碼演算法或協定，建立高效、安全及已驗證為正確之後量子密碼工具程式庫，極大化後量子密碼工具開發與部署效能。

- 實作後量子密碼演算法

  在各種平台(如 X86、ARM、RISC-V 及 FPGA 等)實作後量子金鑰交換、數位簽章演算法及其他以此為基礎之通訊協定。

- 實作後量子通訊協定

  基於後量子演算法所建立之金鑰，進行通訊協定實作。

- 驗證後量子密碼演算法實作

  改良自動化之低階程式驗證工具，並驗證後量子密碼演算法之實作。

(二) 殭屍網路情蒐研析

維運殭屍網路分析系統，蒐集殭屍網路攻擊情資，追蹤分析殭屍網路族群攻擊活動與樣態，研析受駭情資與產製偵測指標，並進行跨域情資分享與聯防，通知受駭單位進行應變處理。

(三) 政府領域網路威脅研析

收容政府骨幹網路流量，建立萃取與威脅分析機制，產製中介分析資料，確保 50% 政府網際服務網骨幹網路流量均納入分析。

建置網路流量威脅分析索引系統，進行政府骨幹網路威脅感知與

分析，提供網路威脅分析能量。

(四) 社交工程情蒐研析

部署惡意電郵陷阱，誘捕惡意程式垃圾郵件(Malspam)散布來源，產製惡意郵件散布來源清單，協助強化機關阻擋過濾各式惡意郵件，提升電子郵件安全。

精進郵件威脅檢測研析技術，產製中繼站黑名單，分享中繼站與惡意電郵情資，強化惡意電郵威脅偵測。

(五) 政府組態基準研究

研究 Ubuntu Linux 22.04 與 Apache Tomcat 10 安全組態基準與部署方式，並檢討與精進政府組態基準發展項目，提供政府機關做為部署之參考，藉由一致性作業系統組態設定，強化資安防護。製作 Windows Server 2022 與 Windows 11 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。

(六) 主動防制技術發展

發展主動式防禦手法相關技術與應用情境，並完成實作驗證，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，提醒政府機關留意攻擊威脅與強化資安防護。透過系統架構精進，提高可同時連線之數量，以及藉由參數調整，加快下達控制命令與回傳控制命令執行結果之速度，提升自動化效率，以強化駭客攻擊技術研究與應用。

(七) 重大弱點研析

持續蒐集資安弱點情資，針對重大弱點進行研析並應用於相關業務，包含對弱點之技術研究，以及當爆發重大弱點時，即時進行衝擊分析並研擬因應策略，如弱點修補方式、緩解措施或檢測工具，並適時發布警訊通知機關即早因應與防護。

(八) 組織型駭侵研析與偵測防護

分析惡意程式之活動與行為特徵，萃取其重要樣態產製偵測規則，並部署於政府骨幹網路進行偵測，同時關聯各項來源情資，以針對特定組織型駭侵族群進行辨識與追蹤。

(九) 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，同時搭配社交工程簡訊與郵件演練，主動發掘潛藏於機關為民服務資通系統弱點，並測試機關人員資安意識，強化資通系統資安防護。

(十)　零信任網路產品功能性檢核服務建置

推動資安產業發展零信任網路相關技術，建立產品功能性檢核平台，發展相關基準與流程，以及提供廠商產品功能性檢核服務，以利政府零信任網路之導入。

五、推動產學合作與技術移轉

依據政府資安需求，研擬產學研合作規範，建立合作管道，並盤點研究成果與預期可供技轉技術項目，研議資安相關技術標準與規範，使研發技術得以落地，推動資安技術應用。業務架構包含「5.1 技術移轉創新育成」與「5.2 政府骨幹網路資料分析實驗場域建置與推動」等 2 項工作項目。

(一) 技術移轉創新育成

針對國家任務導向型研究與關鍵核心研究，自行研發產出具發展潛力與市場價值之成果，透過技術移轉方式，協助國內業者提升技術能力或成立新創公司，並運用經濟部、國發會及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。

依據政府需求，研擬產學研合作規範，建立合作管道。盤點研究成果及預期可供技轉技術項目，研議資安相關技術標準與規範，使研發技術得以落地，推動資安技術應用。

(二) 政府骨幹網路資料分析實驗場域建置與推動

建置政府骨幹網路實驗場域，可供產學合作單位進行網路威脅分析之概念性驗證或服務驗證應用，促進產學合作。

六、研析各國資安趨勢

研析各國資安法規體系，制定政府機關資安規範與指引，並透過資安服務共同供應契約與廠商評鑑改善供需環境生態，以完善資安法規與標準，健全國家資安整體生態體系為目標。業務架構包含「6.1 資安法推動與修正研析」、「6.2 國際資安組織與法制政策研析」、「6.3 政府資安規範發展」等 3 項工作項目。

(一) 協助資安法推動與修正研析

研析國際資安專法規範情形與我國資安法推行議題，依據分析結果提出資安法修正建議。持續研析資安法，以促進適用對象對本法之瞭解、協助法規釋疑作業，並提出相關修法建議。

配合我國資安法檢視其他法律不足之處，本於資安法精神並參酌各國法律發展趨勢，就其他法律進行研析，將資安法精神內化至其他法律中，使其配合資通安全發展，優化國家資安之推動，並據此提出修正方向建議。選定重要法規進行相關研析，以作為政府完善資安法律體系及提升國家資安水平之參考，使我國法律納入「Security by Design」精神，配合數位國家發展，全面提升國家資安防護韌性。

(二) 國際資安組織與法制政策研析

研析主要先進國家與組織之資安推動架構、重大政策與計畫，做為我國研議資安政策之參考。

觀測主要國家對新興議題之政策與法制趨向，並對發展中議題進行追蹤，研析新興或與科技發展、應用相關之資安法制及配套政策議題，並提供研析建議。

建置資通安全法制及政策研究報告之資料庫，分門別類收納相關研究報告與專書等，建立關鍵字及關聯查詢等功能以利查詢、分析統計及延伸利用，以深耕資安政策與法制研究專業領域，強化專業形象與影響力。

蒐集各國產業資安標準，如美國政府採購供應鏈，對比我國相關規定以瞭解其間差異。配合政府需求，選定重要產業進行資安標準發展趨勢研析，提供相關參考資訊協助我國產業進入國際市場。推動我國產業資安標準與國際標準對接，降低產業之非關稅障礙，提高產業國際競爭力。

(三) 政府資安規範發展

依政府資安規範整體發展藍圖，考量外在環境變化與技術發展等因素，編撰或修訂資安相關參考指引，以協助政府機關強化資安管理。

七、擴展國際合作交流

參與國際資安相關重要會議與活動，建立跨國資安情資交流與合作管道，持續加強國際合作夥伴連結，及時掌握全球資安威脅趨勢，並整合國內外資安情資，成為國內主要情資彙整與分享平台。

強化國際資安技術交流，提升國際參與成效，辦理跨國攻防演練，促進國際資安交流與合作。業務架構包含「7.1 國際合作交流」、「7.2 跨國攻防演練」等 2 項工作項目。

(一) 國際合作交流

參與 FIRST、APCERT 及 Meridian 等國際資安組織，爭取擔任督

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，強化跨國資安聯防。

與美洲、歐洲及澳洲等國外學術研究機構進行國際合作，包含跨國前瞻技術研究、參與國際組織進行資安標準制定、辦理(協辦)國際大型學術或技術會議等。增加台灣國際能見度，維繫國際社群關係。

(二) 跨國攻防演練

運用虛擬化平台建置關鍵基礎設施之模擬場域，模擬水資源關鍵基礎設施之資通系統、辦公室環境及網路架構等，並以虛實串接方式，結合資通系統(IT)與工業控制系統(OT)，打造出仿真且完整之水資源工控模擬場域，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，並邀請國內資安團隊及與我國簽訂合作備忘錄(MOU)之國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。

針對駭客實際攻擊手法，透過實作事前之防護部署與情資蒐集、事中之即時處置與損害控管及事後之事件分析與情資分享等，進行經驗交流與建立聯防機制。提供國內外參與者經驗分享與實務探討之平台，提升 2023 跨國攻防演練與會者參與度與活動成效，並促進國際交流。

八、推動資安技術應用

定期檢視政府與關鍵基礎設施之網路與資訊系統安全性，及早發現政府與關鍵基礎設施資安問題，降低資安弱點與設定產生之系統風險。為建構政府安全與韌性環境，建構軟體物料清單、擴充政府設計系統元件與開源碼詮釋資料，盤點民生關鍵資訊系統，執行數位韌性巡防服務，提升整體政府機關資通系統數位韌性。業務架構包含「8.1 資安治理成熟度評估」、「8.2 資安輔導服務」、「8.3 資安服務規劃與廠商評鑑

」、「8.4 資安技術檢測服務」、「8.5 建構軟體物料清單」、「8.6 擴充政府設計系統元件與開源碼」及「8.7 執行數位韌性巡航服務」等 7 項工作項目。

(一) 資安治理成熟度評估

推動政府機關與關鍵基礎設施提供者落實資安治理成熟度機制，並分析資安治理成熟度自評情形，以有效掌握資安成熟度概況。

(二) 資安輔導服務

提供機關資安防護輔導服務，協助強化資安防護措施與落實委外作業安全管理，以符合資安法之法遵義務。

(三) 資安服務規劃與廠商評鑑

檢視政府機關共同供應契約資安服務品項內容，提出相關調修建議，並提供相關諮詢，精進共契資安服務之運作。辦理共契資安服務廠商評鑑，並針對執行情形之回饋意見，調整廠商評鑑內容，精進廠商評鑑機制。

(四) 資安技術檢測服務

協助政府機關與關鍵基礎設施執行資安技術檢測服務，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，以提升檢測能量與成效，同時配合執行資安稽核技術檢測作業與技術檢測專案。

(五) 建構軟體物料清單

蒐集與整理政府資訊系統可利用之開源軟體，對其建立軟體物料清單(Software Bill of Materials,SBOM)記錄構成軟體之元件與關聯表，以具有可讀性之 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。

(六) 擴充政府設計系統元件與開源碼

蒐集資訊專案文件與開源碼詮釋資料，並提供政府機關資訊系統引用相關開源碼之參考資料。

制定專屬網站設計系統，規劃與整理政府系統設計元件庫，透過一致性之設計元件，有效降低使用者學習成本，獲得一致性之服務感受。

(七) 執行數位韌性巡航服務

盤點民生關鍵資訊系統背景資料，推動數位服務設計與數位服務流程再造，協助政府機關規劃資訊系統架構。

擬定年度數位巡航計畫，協助機關診斷資訊系統脆弱點，提出具體改善項目與協助規劃精進措施，並視需要提供技術支援，以協助主管機關盡速落實精進措施，提升整體政府機關資通系統之數位韌性。

九、支援產業資安重大發展

配合國家資安政策分享資安技術，加速資安產業框架與應用情境，提升台灣資安產業之自主能量，積極推動產業導入資安防護機制，以確保我國整體資通安全。業務架構包含「9.1 支援產業資安發展」工作項目。

(一) 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。

1. 產業資安投資狀況調查

配合政府需求，選定重要產業進行調查，依據該業種內之企業規模，透過對資訊或資安主管進行訪談或問卷調查等方式，蒐集企業之資安投資項目、金額、人力及企業營運情況，以及內外部環境

對於資安投資之影響等相關資料。依產業投資資安之要素，研擬鼓勵產業投資資安之策略，提升產業資安防護能量，強化產業資安韌性。

2. 擬定產業資安投資建議

配合政府需求，選定重要產業為對象，依據該業種內之企業規模，針對其所涉及資料種類、採用資訊系統類別與複雜度、面對之風險類別、規模及損害嚴重性，並考量企業資源分配，進行相關研究與分析，提出各產業之資安投資建議。協助產業進行資安投資，掌握投資規模與優先項目，作為鼓勵產業投資資安策略之決策支援，以有限資源最大化產業資安能量。

十、培育資安人才

因應國家發展需求，為充實各領域資安人才，設置資安人培實體場域，強化工控領域訓練，並設置虛實整合競賽平台，提供學習與演練管道，孕育優質資安人才。業務架構包含「7.1 資安職能訓練」、「7.2 資安人才培育」、「7.3 資安人才評量」及「7.4 資安高階人才養成」等 4 個工作項目。

(一) 資安職能訓練

1. 資安職能訓練課程開發

持續推動資安職能訓練，完成 2 項進階課程教材開發，並滾動檢討已開發之課程教材內容。

依照資安職能地圖持續擴充資安課程，提升資安人才培育成效，擴大資安人力供給。

2. 推動資安職能訓練機構遴選制度

推動資安職能訓練機構遴選制度，評估資安職能訓練需求，認證資安職能訓練機構，擴大資安職能訓練量能。

(二) 資安人才培育

進行調查研究，掌握產業資安人才需求狀況，依據缺口建立對應之培育策略。

發展頂尖產業資安人才(含政府人員)培訓實作環境，培育國內高階實戰人才。

(三) 資安人才評量

精進資安職能訓練評量機制，檢討評量試題品質，並依資安職能訓練課程進行評量試題命審作業。

設置資安技能檢定場域，提供多元且即時資安技能檢定模式。建置離線版評量作業模式，提升評量作業穩定性與可用性。

(四) 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)。

維運資安攻防平台，並擴充攻擊劇本及相關測驗等功能，以提供受試者正確掌握相關技能，並應用於日常維運工作中。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

持續開發以藍軍為核心之紅藍攻防實戰平台腳本，提供線上學習與演練管道，加強紅藍隊頂尖人才訓練及養成。

招收企業、法人與政府機構之資安資深人員，因應國內資安政策方向及新興資安議題，對資安專責人員開設進階課程。除課程外

，每期將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，掌握關鍵資安技術之高階資安菁英人才，強化單位資安防護能量。

3. 開發自主實戰訓練教材

初期參考國外頂尖資安課程，如 SANS NetWars，議題涵蓋網頁安全(Web Security)、行動裝置安全(Mobile 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)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，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。

招收具資安專長之特定對象，與如 HITCON 等資安社群合作，進行資安專業課程訓練，作為國手代表國家參與各種資安競賽，提升國家於資安領域之國際能見度。強化選手技術，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，協助參與國際競賽。

十一、推廣全民資安意識

辦理政府資通安全防護巡迴研討會與資安競賽，與相關部會合作透過資安政策宣導及資安威脅趨勢與案例分享，強化政府機關資安意識，提升政府機關資安人員之資安技術與管理能力，並藉由不同主題活動、遊戲及競賽等方式，推動資安技能向下扎根，強化全民資安意識，提升資通安全之素養與水準。

針對最新資安案例進行研析，評估並摘選重要資安相關法規加以彙編，或編撰相關文件，以提升機關對資安法規之瞭解。業務架構包含「11.1 資安系列競賽」、「11.2 資安法規與案例彙編」等 2 項工作項目。

(一) 資安系列競賽

辦理全民資安意識系列活動，嘗試社群經營、活動、遊戲及競賽等方式，進行全民資安通識訓練與推廣。結合外部資源推動跨域應用資安教育：吸引各界人士及國際資安組織串連參與，推廣全民正確資安意識與認知。

(二) 資安法規與案例彙編

研析最新資安案例，並提出法律分析與管理建議，以提升機關對資安法規之瞭解。評估並摘選重要資安相關法規加以彙編，或編撰相關文件，以供機關參考利用。

參、年度目標

本院 112 年度業務各工作項目之年度目標，詳見表 1。

表1　工作項目年度指標

業務計畫	工作項目	年度目標
1. 推動資安防護機制	政府領域聯防監控	訂定政府領域聯防監控情資格式，導入 STIX 2.1 標準格式，產製聯防監控情資
	資安情資分享	▪ 強化國際情蒐合作，增加全球共通性資安情資 ▪ 規劃開放情資分享，提供學研單位或國際資安組織參考
	資通安全弱點通報	協助 C 級公務機關及關鍵基礎設施提供者完成導入資安弱點通報機制

業務計畫	工作項目	年度目標
	零信任網路資安防護	協助推動 2 個機關導入零信任網路之設備鑑別機制
	端點偵測資安防護	協助推動 A、B 級公務機關導入端點偵測及應變機制，並接收偵測結果進行分析
	政府領域威脅戰情資訊掌握	彙整政府領域資產威脅與網路攻擊情資，掌握政府資安威脅與防護情形
	誘捕偵測資安防護	協助推動 2 個資訊資源向上集中機關導入內網威脅誘捕機制
	黑名單自動化阻擋	協助推動資訊資源向上集中之 2 個機關導入黑名單自動化部署機制
	惡意電郵偵測防護	協助推動資訊資源向上集中之 2 個機關導入惡意電郵偵測機制
	關鍵基礎設施資安防護技術支援	推動各關鍵基礎設施領域擇 6 個 A 或 B 級關鍵基礎設施提供者，導入國家層級資安風險評估機制
2. 執行重大事件應變處置	資安通報與諮詢	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	▪ 推動 N-CERT 事件通報資料交換機制 ▪ 持續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

業務計畫	工作項目	年度目標
3. 支援敏感性政府機關資安防護	重點機關資安監控與防護	產製重點機關資安服務月監看報告，共計 12 期
4. 研發資通安全科技	資安前瞻研究	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
	殭屍網路情蒐研析	追蹤殭屍網路威脅，分享 12 次殭屍網路偵測指標與分析情資
	政府領域網路威脅研析	▪ 建置政府骨幹網路流量分析平台，建立萃取與威脅分析機制 ▪ 建置分析索引系統，進行網路威脅感知與分析
	社交工程情蒐研析	產製中繼站黑名單，分享 50 次中繼站與惡意電郵情資
	政府組態基準研究	發展「作業系統」與「應用程式」類別電腦組態基準
	主動防制技術發展	精進主動式防禦應用平台自動化效率，並持續實作驗證 2 套攻擊情境
	重大弱點研析	關注重大弱點與發布警訊，每年完成至少 2 個重大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，每年完成產出 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

業務計畫	工作項目	年度目標
	零信任網路產品功能性檢核服務建置	完成 5 家廠商產品功能性檢核服務
5. 推動產學合作與技術移轉	技術移轉創新育成	推動 2 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 1 個政府骨幹網路實驗場域
6. 研析各國資安趨勢	協助資安法推動與修正研析	協助滾動檢討修正資通安全管理法及子法，提出 1 項修改建議草案
	國際資安組織與法制政策研析	研析 8 個國際資安組織或國家之法制政策
	政府資安規範發展	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
7. 擴展國際合作交流	國際合作交流	▪對接國外資安技術或研究機構累積達 3 家，持續接軌國際同時提升台灣資安研發之能見度 ▪辦理(協辦)1 場國際大型資安學術或技術會議，參與人數至少 200 人
	跨國攻防演練	辦理 1 次跨領域(或跨國)關鍵基礎設施攻防演練
8. 推動資安技術應用	資安治理成熟度評估	▪推動 30 個 A 級政府機關落實資安治理成熟度(含客觀指標)達第 2 級以上 ▪推動所有 A 級關鍵基礎設施提供者工控資安治理成熟度達第 2 級以上
	資安輔導服務	每年遴選 10 個機關進行實地輔導，並落實委外作業安全管理

業務計畫	工作項目	年度目標
	資安服務規劃與廠商評鑑	每年完成資安服務廠商評鑑作業
	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
	建構軟體物料清單	每年整備(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源碼	▪每年調校(新增與編修)政府系統設計元件 10 案 ▪每年完成資訊專案文件與開源碼詮釋資料中文化 5 案
	執行數位韌性巡航服務	▪至少 3 項民生關鍵資訊系統以及 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 ▪完成數位韌性領航員訓練課程至少 6 名 ▪招募或委託技術人員約 33 人至 47 人，專職辦理政府安全與韌性環境服務任務與工作內容
9. 支援產業資安重大發展	支援產業資安發展	辦理 1 場技術交流活動，與各界分享國際間相關技術發展資訊
10. 培育資安人才	資安職能訓練	▪持續完成 2 個資安職能構面訓練課程開發 ▪推動調訓機制，培訓政府機關專職人力達 200 人次以上
	資安人才培育	培育國內高階實戰人才 125 位
	資安人才評量	發展頂尖產業資安人才培訓實作環境(如增加紅藍攻防平台腳本)

業務計畫	工作項目	年度目標
	資安高階人才養成	▪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 ▪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 ▪建立自主頂尖資安實戰課程，並邀請國外資安學界、業界及社群知名人士培訓國內實戰人才至少 125 人次
11. 推廣全民資安意識	資安系列競賽	實體各項競賽與活動全年 650 人次
	資安法規與案例彙編	完成資安法規、資安法律案例彙各 1 本

資料來源：本院整理

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。112 年度政府補助預算收入計 890,318 千元(經常門 820,318 千元、資本門 70,000 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 3 億 12,576 萬元。

二、業務費用

業務費用經費預估 519,268 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 149,187 千元

；電腦軟體服務費用 198,460 千元；委託調查研究費用 62,832 千元；勞務委外費用 95,721 千元及其他業務費用 13,068 千元。

三、資本門費用

固定資產建設改良擴充費用經費預估 70,000 千元，為執行業務所需，採購或汰換更新設備相關費用預估 67,376 千元，以及採購/汰換辦公事務設備及電信設備(如電話交換機、投影機、印表機、視訊會議系統、網路攝影機主機及投影機等)預估 2,624 千元。

表2　112 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	312,576	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 3 億 1,257.6 萬元，年平均人事費 142.1 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、全民健康保險費、勞工退休金，計約實際薪資 47.7%，故年平均實際薪資為 96.2 萬
服務費用	445,548	▪ 電腦軟體服務費預計 198,460 千元，包含惡意程式檢測分析、端點安全防護機制、政府骨幹網路威脅分析機制、鑑識分析使用、虛擬桌面平台授權、防火牆政策分析工具、零信任網

金額單位：千元

科目及營運項目	預算	說明
		路身分鑑別、跨國攻防演練環境建置使用、跨國攻防演練場域紅藍隊主機監控、資料庫同步資料模組、系統開發與測試軟體授權及各項雲端服務費用等 ▪委託調查研究費預計 62,832 千元，包含委託外界研發、委託資安人才供需調查、委託產業資安投資調查及委託國民資安意識調查等 ▪勞務外包費預計 95,721 千元，包含跨國攻防演練活動、資通安全法律及案例彙編、資安弱點通報機制實作訓練、課程開發、政府資通安全防護巡迴研討會、資安系列競賽、辦理國際研究會議、行政系統建置、標準定期驗證費用等各項勞務外包 ▪國內外出差相關費用預計 38,414 千元，包含國外出差、出國考察交通費、生活費等費用共 90 人次出差費用及推估 220 人年國內差旅費用 ▪資訊設備修繕養護費及保固費用預計 25,629 千元，包含政府骨幹網路資料萃取機制設備、網路封包中介設備、網路分流設備及 VSP-G400 儲存設備、工控場域設備維護無線網路基地台設備維護、Sentinel 設備維護、垃圾郵件設備維護、防火牆設備維護、伺服器與儲存設備維護等 ▪水電與郵電相關費用預計 20,211 千元，包含辦公場所水電、電話及數據通信費等

金額單位：千元

科目及營運項目	預算	說明
		▪其他費用預計 4,281 千元，包含印刷裝訂及廣告費、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)及公共關係費等
材料及用品費	3,100	▪報章什誌：資安相關標準、資安專業雜誌、國內外期刊預計 1,448 千元 ▪使用材料費：為設備運轉、維護所耗用之物料預計 150 千元 ▪用品消耗費：文具用品、書報雜誌及其他一般事務費預計 1,502 千元
租金及利息	23,350	▪各項活動場地租金預計 4,011 千元 ▪維運所需之機器設備、電信機櫃租用費用租金預計 11,339 千元 ▪房租：辦公處所租金費用預計 7,000 千元 ▪什項設備租金：辦公事務影印機等設備租賃費用預計 1,000 千元
稅捐與規費	1,213	▪消費與行為稅：各式契約等憑證貼用之印花稅票預計 1,073 千元 ▪規費：政府機關各項規費費用預計 140 千元
會費、捐助、補助與分攤	21,463	▪分攤：分擔辦公處所大樓管理費用預計 1,108 千元 ▪參加國內外組織會費 291 千元 ▪對國內外團體與個人之捐助及獎助學生公費贊助款 20,064 千元

金額單位：千元

科目及營運項目	預算	說明
其他費用	10,264	▪員工教育訓練費、保全費及環境清潔費等預計 11,316 千元 ▪辦理各項活動、演練及研討會等之會議費用 1,752 千元
小計	871,914	
資本門(固定資產建設改良擴充費用)		
機械及設備	67,376	執行業務所採購或汰換更新設備相關費用，預計 67,376 千元，包含政府骨幹開源流量分析建置、部署向上集中機關誘捕機制、資安威脅分析工具與 ARM 平台分析、資安威脅視覺化展示工具、惡意程式檢測分析、跨國攻防演練 2023 場域環境儲存使用、分析向上集中內網誘捕機制日誌、政府骨幹網路威脅分析機制及資安檢測使用等資訊電腦設備等
交通及運輸設備	1,434	採購電信設備相關費用預計 1,434 千元，包含電話交換機等
什項設備	1,190	採購/汰換辦公事務設備相關費用預計 1,190 千元，包含投影機、印表機、視訊會議系統、網路攝影機主機及投影機等辦公事務設備等，以及滅火器、火警授信總機及警防機具等設備
小計	70,000	
合計	890,318	

資料來源：本院整理