「法務部調查局多雲資安戰略數位升級」
中程計畫(114 年至 117 年)
（核定本）

中華民國 113 年 6 月

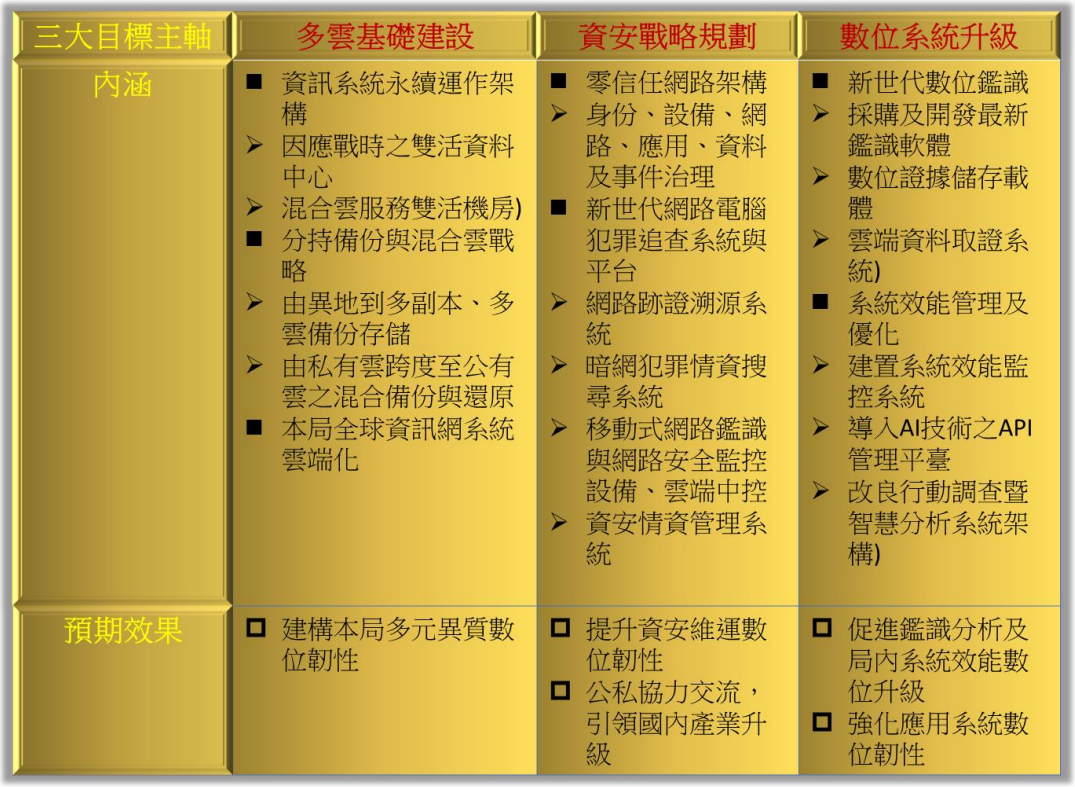
目錄

壹、計畫緣起

本局依法務部調查局組織法，職掌國家安全、重大犯罪調查及辦理電腦犯罪防制、資安鑑識及資通安全處理等事項，且基於我國已連續九年遭受全球高頻率及高密度假訊息及資安攻擊，若發生例如俄烏戰爭或臺海兩岸局勢緊張時，敵方為積極抑制或斷絕我國情資蒐取及戰略因應能力，勢必優先擇定政府機關、關鍵基礎設施等單位作為首要及密集目標，利用分散式阻斷服務(DDoS)及生成式人工智慧(AI)等資訊新興科技發動網攻，以遂行癱瘓我國國安與社安而獲致戰果。觀諸國家數位韌性之關鍵，即在於政府能將受攻擊或被摧毀的實體網路通訊等硬軟體關鍵基礎設施所提供之數位服務及所保存之公共資料，藉由早已異地完整保存於例如雲端設備之資訊備份進行快速重建復原、透過網路為民眾提供必要服務而確保政府功能連續性與正常運作。然盱衡本局現有維運中之各式關鍵基礎設施、軟硬體系統、平台及應用程式未與時俱進，若無法及早導入各項治理、服務及儲存雲端化、異地分持備份、AI、加密運算等相關新興資訊技術以具體執行「多雲基礎建設、資安戰略規劃、數位系統升級」目標，實無法有效達成「戰時應變」、實踐「資安即國安」戰略及因應 AI、AIoT、5G 或量子電腦時代來臨衍生之各項挑戰並取得數位韌性成果，亦無法有效縮減資料維護及系統效能維運成本。

鑒此，本局綜整所屬機關需求，提報本計畫爭取經費，以「多雲基礎建設」、「資安戰略規劃」及「數位系統升級」三項目標主軸，運用雲端機房分持備份、多雲與混合雲技術，建置本局全球資訊網系統升級雲端化，並基於主動防禦、網路防控、資安應變之策略與方式，將各式資訊系統予以建置或擴充，以符合資安戰略需求，且導入 AI 及後量子密碼學加密技術(PQC)等新興資訊技術優化與提升鑑識軟硬體及各管理系統效能，期使服膺「數位韌性政府」與「資安即國安」戰略並完成數位系

統升級及提升科技支援刑事偵查能量。



三大目標主軸	多雲基礎建設	資安戰略規劃	數位系統升級
內涵	■ 資訊系統永續運作架構 ➢ 因應戰時之雙活資料中心 ➢ 混合雲服務雙活機房) ■ 分持備份與混合雲戰略 ➢ 由異地到多副本、多雲備份存儲 ➢ 由私有雲跨度至公有雲之混合備份與還原 ■ 本局全球資訊網系統雲端化	■ 零信任網路架構 ➢ 身份、設備、網路、應用、資料及事件治理 ■ 新世代網路電腦犯罪追查系統與平台 ➢ 網路跡證溯源系統 ➢ 暗網犯罪情資搜尋系統 ➢ 移動式網路鑑識與網路安全監控設備、雲端中控 ➢ 資安情資管理系統	■ 新世代數位鑑識 ➢ 採購及開發最新鑑識軟體 ➢ 數位證據儲存載體 ➢ 雲端資料取證系統) ■ 系統效能管理及優化 ➢ 建置系統效能監控系統 ➢ 導入AI技術之API管理平臺 ➢ 改良行動調查暨智慧分析系統架構)
預期效果	□ 建構本局多元異質數位韌性	□ 提升資安維運數位韌性 □ 公私協力交流，引領國內產業升級	□ 促進鑑識分析及局內系統效能數位升級 □ 強化應用系統數位韌性

一、計畫依據

（一）依行政院第六期「國家資通安全發展方案(110 年至113 年)」之「善用智慧前瞻科技、主動抵禦潛在威脅」推動策略，優先於資通安全責任等級 A 級公務機關導入零信任網路資安防護環境，貫徹「資安即國安」戰略，完善政府網際服務網防禦深廣度，並執行「提升科技偵查能量，防制新型網路犯罪」等具體措施，以強化新型態網路犯罪之偵查能量、提升資安事件溯源追蹤能力及加強跨境網路犯罪偵查機制。

（二）依行政院智慧國家推動小組提出「智慧國家方案(2021-2025 年)」項下規劃之數位基盤建設，針對亞太海纜及 5G 雲端聯網中心，完善在地光纖通道、強化安全防護，讓臺灣成為國際資通中心樞紐，為邁向智

慧國家奠定基礎。

（三）依國家發展委員會前瞻計畫「強化公部門網路服務與運算雲端基礎設施計畫」目標二「雲端服務之韌性與品質提升，對外服務利用資訊系統雲端化，優化服務韌性及品質，並建立雲端服務管理制度，提升服務營運效益」，將本局全球資訊網系統資料及應用服務依公開或機敏屬性逐年透過所建置雲端安全鏈路達成雲端化存取與傳輸，並建置與維護 DDoS 攻擊防護功能，以防阻外部非法駭侵攻擊、實現數位韌性及因應未來風險。

（四）依「資通安全責任等級分級辦法」第 4 條第 2 款「業務涉及外交、國防或國土安全事項」，行政院核定本局為資通安全責任等級 A 級機關，據以辦理資通安全管理法各項規定事項及資通系統分級安全控制措施，以強化本局整體資安防禦能量。

（五）依資通安全管理辦法第 10 條「公務機關應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫」及資通安全管理法施行細則第 7 條第 1 款「一、公務機關依其組織法規，足認該業務為機關核心權責所在。」，故重要資訊業務應該採取必要的安全措施以確保資訊安全，包括資料異地備份，且該機關應提供符合使用者需求之服務品質及可用性，於實施數位韌性政府確保系統之高可用性及彈性，以應對災害及緊急情況並確保資料之完整性及持續性，本局據此辦理既有系統、API 管理平台及行動調查暨智慧分析等系統之擴

充、效能監控及優化、資料異地備份及全球資訊網系統建置分散式阻斷服務攻擊防護、雲端移轉、作業系統維運、系統變更開發等升級雲端化安全措施。

(六)依行政院科技部「臺灣資安卓越深耕-先進網路鑑識計畫-網路跡證溯源子計畫(110-113)」之「精進科技與訓練，支援蒐證、反蒐證、通訊監察與電腦犯罪防制等科技監察與蒐證工作，貫徹犯罪查緝及肅貪之政策」推動計畫，以自動化、科技化系統迅速蒐整網路中犯罪資料，分析手法及模式，輔以隨案件偵辦累積之執法專用資料庫，建構預警機制及提升調查溯源效能。

(七)依法務部 113 年度目標一「推動司法改革政策，提升鑑識證據品質,AI 輔助強化檢察功能」之策略(三)「推動法務服務智慧轉型，建構數位化科技辦案及創新服務環境，強化資訊安全體系，優化法務行政效能；透過 AI 協助協助檢察官進行案件之證據辨識」與目標四之策略(三)「建構嚴密之安全防護網，提升安全防護工作，調查、溯源及防堵錯假訊息，並強化偵辦能量，機先防制及發掘境外敵對勢力，或其他非傳統安全危害等狀況，以維社會安定；防制境外敵對勢力之滲透干預，偵處意圖危害國家安全及社會安定之個人或組織，防範高科技營業祕密被竊，以維護國家高科技產業競爭優勢，運用科技創新研發，發揮鑑驗偵防科技量能」,藉由各項資源的投入,精進本局科技偵蒐與鑑識技術，強化鑑識、電腦犯罪防制與科技蒐證量能並實踐犯罪查緝。

(八)依「中華民國科學技術白皮書(112 年至 115 年)各機

關（單位）科技發展中程目標」之數位韌性總體目標3「建構軍民通用的科研體制，整合公私科研量能，發展尖端戰略科技及自主國防產業」及總體目標6「兼顧軟體與硬體的韌性社會基礎建設、維運及研發，強化敏捷應變體系，因應未來風險管理」。

（九）依「國家科學技術發展計畫(民國110年至113年)」有關法務部提出之目標：1.引進先進科學鑑識科技，建構尖端鑑驗技術，提升鑑識品質與成果效益。2.提升科技，支援蒐證、反蒐證、通訊監察與電腦犯罪防制等科技監察與蒐證工作，貫徹犯罪查緝及肅貪之政策。3.建立科技工作特色專長支援調查保防。4.建置行為科學鑑識網絡，促進肅貪案件偵辦效能。

二、未來環境預測

兩岸及國際情勢詭譎，資安威脅型態瞬息萬變，俄烏戰爭善用雲端架構及資料數據中心事例可茲各國借鑒，我國政府機關基於「資安即國安」戰略思維及雲端備份與回復策略，亦應完善緊急及戰時透過多雲基礎建設快速完成重建、復原與提供服務之能力。既有資訊系統及資料之數位韌性需求與未來環境預測，可由「多雲基礎建設」、「資安戰略規劃」及「數位系統升級」三項主軸配合雲端化、AI及後量子密碼學加密等新興資訊技術發展，綜合預估如下：

（一）以多雲基礎建設重構關鍵設施及全球資訊網系統，型塑數位韌性政府：

1.關鍵設施於戰時易淪攻擊目標，考驗數位韌性：

俄烏戰爭中，俄羅斯除以軍事武器轟炸烏克蘭政府與民間實體建築設施外，亦發動網路攻擊企圖癱瘓烏國政府運作與民間經濟活動，烏克蘭政府即提早將政府及民間公共或重要關鍵資訊訊息及其加密備份

資料透過公有雲或位於各地的數據中心儲存，因此於戰時即可成功維持其軍事行動和民生營運，令敵方實體武器與虛擬網路攻擊對政府運作影響得以降至最低，且將服務移入雲端後，不僅業務得以存續，也縮短了資料維護與營運成本。從而，我國面對兩岸關係的高度不確定性及長期遭受假訊息網攻之現況，應及早強化關鍵建設並透過科技投資因應日漸升高的衝擊風險。藉由多雲基礎建設架構使機關關鍵設施得以具備數位韌性，例如建置跨地緣政治風險的雲端儲存策略、雙活機房、公有雲備份分持、混合雲加密資料備份及資料與應用伺服器介接系統等，當機房毀損時資料及系統服務即可迅速自雲端復原，確保機關多元異質數位韌性能及時應變各類風險。

2.傳統主從式架構資訊系統不具快速復原之數位韌性：

虛擬戰爭中，駭侵者利用假帳號、中繼站發動網攻，穿透受攻擊之政府機關防火牆、製造瞬時異常封包流量以癱瘓郵件等伺服器系統、全球資訊網服務、竊取或毀損所儲存公開或機敏資料，相較之下，傳統主從式架構資訊系統環境欠缺快速復原之數位韌性，致使嚴重影響政府運作，故我國政府機關應及早建置、轉換為多雲、混合雲之雲端服務架構與安全傳輸鏈路，以期因應戰時及緊急時之業務存續與資料維護等需求。

3.全球資訊網系統應進行雲端化升級及具備防禦 DDoS 攻擊能力：

依國家發展計畫及公部門推動方向，政府機關所屬系統進行數位轉型可由雲端服務、大數據應用等數位應用領域提供服務並創造新機會與可能，而雲端服

務是一項結合雲端運算、雲端儲存及網路連線與管理之網際網路服務，可彈性因應各雲端服務之連線、運算及資料測量變動，快速且彈性部署所需網路頻寬、伺服主機、微服務叢集及資料空間。是以，本局全球資訊網應積極依據資料屬性、存儲及傳輸交換風險程度，憑藉雲端資安戰略下所建置安全資料鏈路雲端服務可擴充性及可靠性之特性，進行資料分持存儲及制定備份回復及網路攻擊防禦措施，使得網站服務及營運不中斷且能量得以再提升，並強化服務韌性及品質，逐步達成雲端移轉與維運等網站雲端化近程與目標。

（二）零信任網路架構治理及網路犯罪追查系統應納入資安戰略規劃、提升資安維運數位韌性：

1. 零信任網路架構涵蓋面尚未擴及身份、設備、網路、應用、事件及資料治理：

既有安全模型建立於「網路中所有內容都可供信任」之假設前提已然過時，因此，零信任網路架構除應涵蓋身份及設備治理，亦應涵蓋網路、應用、事件及資料治理，即需要將例如解決未知或有安全疑慮的人員、網路移動行為、設備於使用或連結內網權限問題，有效管控應用程式開發、部署、使用和維護於安全、可靠、合規與高效環境中運行，且對事件記錄、告警及自動化處理以減少人力監控及處理時效，及對機敏資料正確性及不被竄改性進行確保等身份、設備、網路、應用、事件及資料治理項目均予納入資安戰略。

舉例而言，未全面涵蓋於零信任網路架構且納入資安戰略所遭遇缺乏數位韌性現況及可能作法，包括：

(1) 隨著自動化及 AI 技術在各行業及資訊環境之發展與普及趨勢，包含本局之數據與資訊在線上與離線環境之儲存、傳遞、散佈、蒐集及利用等行為所導致之安全風險均將提高，致使需要更強大的資訊安全系統來保護單位的數據和資產之需求將與日俱增。

(2) 智能裝置和物聯網泛用之關鍵基礎設施環境及應用軟硬體系統，易形成資安攻擊弱點及破口，資安機關及防護單位勢將首當其衝、面臨更多、頻繁、多樣化之攻擊型態，因此需要更強大的安全系統來實施該些裝置與相關數據之防護。

(3) 攻擊者技術和策略不斷演進，勢將出現前所未見之威脅與攻擊方式，本局需及早準備以應對新型態資安攻擊事件與類型，並有相應安全系統來檢測與防止。

(4) 因疫情及景氣循環等原因，促成遠距工作與行動辦公興起與蔚為風潮，本局的公開或非公開資訊、數據或公文可能會在不同的網絡和設備上進行傳輸、交換與存儲，無疑增加了資訊外洩和違規行為的風險，需要有相應的安全系統確保資訊的安全。

(5) 因應數據隱私與資訊安全法律規範陸續制定與發佈，政府與監管機構勢將加強稽核法律合規性之

要求，本局須建置妥適完善的安全系統以確保所屬人員能切實落實法遵規範。

(6) 本局因業務機密性與維護國安與資安重責之特殊性，競爭對手為竊取國家安全機密或技術信息，勢必會將本局作為主要資安攻擊目標與實施間諜活動之對象，以遂行其目的，惟有建置與維運具有資安戰略思維之強大資安系統，始可防杜所述風險及破解不法意圖與行為。

2.基於主動防禦、網路防控、資安應變之資安即國安戰略，積極開發資安系統：

(1) AI 生成多媒體型態錯假訊息比例上升：

自 2018 年美國華盛頓大學研究團隊發布一份以 AI 技術生成美國前總統歐巴馬演講影片之研究，迄今可看出相關技術已取得顯著的進步；近年來，例如 OpenAI ChatGPT、Microsoft Bing AI 及 Google Bard AI 等以 AI 技術為輔助之自然語言處理技術應用與服務，其能依照使用者需求自動生成文章及合成特定人物或事物之影片，且所生成之肉眼幾難察覺爭議偽變造訊息內容，非透過科技軟體輔助檢驗幾乎難以分辨是否由人類撰寫或生成，此難辨真假之現況亦構成惡害假防制困難，故顯見未來 AI 技術應用於日常生活、改變現今環境已是必然趨勢，且持續發展溯源系統有其必要性。

若境外勢力或有心人士透過 AI 生成「同樣意旨，然寫法相異」之錯假訊息，使執法單位難以透過「關鍵字排列組合」進行蒐整，將大幅降

低執法單位查獲異常社群組織之機會，故本局為因應新興科技衍生之犯罪問題及偵查需求，持續研發並升級「網路跡證溯源系統」俾利犯罪調查之加值服務，達成間接提升國內科技開發公司自主研發 AI 能量並締造科技偵查及經濟發展雙贏局面，即屬可期；併考量反制爭訊系統之建置與AI 技術之導入，主要元素為「廣大資料源」、「強大硬體運算效能」等，若由執法單位分別建置，將有重複流程、項目等預算花費，故倘能在跨機構聯合建置下，由各單位提出「系統功能需求、資料源涵蓋標的需求、實務需求」，委託廠商或具技術能量之政府單位主責建立「大容量資料庫」，即可匯集可觀預算共同建置強大硬體運算效能之資料庫及伺服器，在爬取、解析、儲存網路資訊達成統合之綜效，提升所述網路跡證溯源系統資料可用性及輔助偵案效能。

(2) 封包傳遞多層次匿蹤阻礙司法調查：

科技的高速發展帶來許多的便利，卻也同時為犯罪份子提供新犯罪機會及手段。本局在偵辦新型態科技犯罪案件如網路詐騙、竊取重要資訊等，不僅在數量上逐年增加，又因為犯罪份子可透過現有匿蹤軟體技術阻礙調查，使得司法人員將面臨前所未有的挑戰，如何偵查則成為一個重大的議題。黑暗網路又簡稱暗網，常透過 Tor(洋蔥路由)進行訪問，因封包內容會經過多層次加密，使有心人士能自訪問網站時身分及位置能始終保持匿名，近年比特幣、太達幣等虛擬貨幣興起，亦使我國執法單位無法以人工進行逆向追查，

故本局為因應新型態科技犯罪之偵查需求及提升辦案之能效，希能持續訂閱暗網搜尋工具服務，持續透過其人工智慧輔助分析，從中勾勒犯罪集團在暗網之行為及模式，賦予第一線科技辦案同仁打擊犯罪之利器，以維護國家安全、穩定社會發展，並藉由偵查方式改良升級，有效解決多層次匿蹤之偵查難題。

(3) 刑事偵查側錄封包量致系統資源不足：

近年隨著人們對於資料儲存及價格上的考量，使用者逐漸從傳統機械硬碟更換為傳輸速率更快、儲存容量較大之儲存設備，雲端服務供應商亦不斷提升網路頻寬，以供更多使用者連線，使得側錄刑事偵查當事人電腦或伺服器等電子設備所得封包量變得相當龐大且更為耗時，軟體、硬體設備系統效能趨於不足。

(4) 情資蒐報系統需可掌握特定情資、減少溝通時間及提高情資採用率：

本局為我國犯罪偵查與情報蒐集機構，資安情報具獨立性、專業性及隱蔽性，需仰賴內外勤人員相互配合統整及蒐報有利於案件查辦相關資安情資，外勤情報提供人員除須培養自身資訊相關涵養，釐清本局蒐報方針外，亦須廣結業界及轄內具資安背景友人，始能取得即時且具關鍵性資安情報；內勤審核人員除需具備高於外勤情報提供者資安技術及更深厚的人脈外，亦須理解目前國家及上級機關整體政策方向，始能審核外勤提報資安情資給予指導，另能配合政策及交查訂

定合理本局合理蒐報方針。是以，有鑒於資訊及資安相關政策變動快速，本局需建立更具彈性的平台，用於制定及交查相關特定情資；另應針對所需蒐報必要項目制定表類，以利外勤情報提供者能提報符合需求情資，減少情資溝通時間，提高整體情資採用率。

（三）以新興資訊科技促進鑑識分析及局內系統效能數位升級、強化應用系統數位韌性：

1. 案關數位跡證鑑識應採用最新數位鑑識軟體及版本更新：

隨著晶片製程更迭迅速，個人電子產品已成為生活中不可或缺的配備，蘊藏個人資訊及網路世界數位足跡，足以勾稽日常活動、社交情形、歷史紀錄及相關犯罪跡證。在本局重大犯罪偵辦實務上，自當事人持有之手機或電腦等裝置擷取數位證據，時常成為案件突破點及關鍵證據，影響甚鉅。近年裝置硬體效能及儲存容量不斷提升，手機主流容量自 106 年 64 GB 成長至 112 年 256 GB 版本，而現今電腦固態硬碟普及且價格實惠下，電腦主流容量則常見 1T 至 2T，推估未來至 117 年仍持續增長；於鑑識層面上，處理巨量資料耗時費工，載入擷取資料分析亦面臨硬體效能不足之困境，造成鑑識效率逐步降低，亟需同步採購最新高效能鑑識工作站及建置自動化案件處理排程，方能提升鑑識效率。

本局於 106 至 109 年間陸續建置六都數位證據檢視分析室，強化數位證據自主檢視分析能力，加深本局第一線人員辦案量能，惟距本計畫首年已逾 5 至

8 年，其鑑識設備之硬體效能恐逐漸不敷需求使用，亟需汰舊換新以符合現今鑑識需求；復因 112 年本局將 TAF 認證 ISO/IEC 17025 資安鑑識實驗室測試場域延伸至南部地區，成立高雄資安鑑識實驗室，擴增本局資安鑑識實驗室人員編制，平衡北南部鑑識資源及量能，並加速中南部地區取得鑑定報告之時效；考量該實驗室成立後，預估鑑定業務量持續增長，鑑識軟硬體設備及鑑定人員額亦將同步提升，遂有新購置軟硬體之需求，方能發揮本局資安鑑識最大功效。

根據資策會產業情報研究員調查，預估 112 年全球手機出貨量 13.27 億台，未來受到 5G 通訊影響，帶動手機出貨量仍持續成長。近年本局收案證物類型以手機為大宗，分析所得之數位證據至關重要，如多媒體檔案(照片、影片等)、對話紀錄、社群媒體使用歷程、聯絡人資訊等，均能精準掌握涉案對象數位足跡，攸關取得案情突破及犯罪事實之關鍵，使犯罪者無所遁形。因此，擷取及分析手機證物儼然成為當今數位鑑識亟待解決之課題，歸因於各手機廠牌新機款式眾多、產品汰換週期短，且手機韌體版本數以萬計，衍生鑑識軟體支援度不一等問題；另有鑑於不同軟體能解析之資料類型各有差異，僅憑單套軟體難以處理分析大部分市面上常見手機，且手機作業系統版本更新迅速，各鑑識軟體間往往淪為追逐競賽，必須隨時保持最新版本及確效，方能有效擷取出案關資料，遂有購置多款鑑識軟體及延續軟體授權之需求，以產出公正、客觀、專業及優質之鑑定報告，成為有效之法庭證據，毋枉毋縱。

2.核心應用系統需持續有效管理、升級及優化：

本局既有核心應用系統為了因應數位升級、優化系統效能及偵查需求，也為了能夠提供行動調查系統穩定維運及使用新技術的查詢方式，管理者需要有效率地開發並管理龐大的程式碼專案，也必須逐年擴充應用伺服器數量，所衍生的後續維運及管理複雜度大幅提升等系統效能管理與優化問題，若無配置有效的管理工具供伺服器發生問題初階段即予以及時排除，待伺服器因問題累積致失能、無法再提供服務時，應用系統隨之失效將導致本局相關業務被迫中斷。各網站間以API作為資料交換的方式,相較於傳統單純FTP資料介接，此不失為兼具安全性及便利性的開發方式，然而，隨著 API 數量因應數位升級而增加，管理者需要有效管理既有及開發新的API且進行系統效能管理。

三、問題評析

（一）關鍵設施及全球資訊網系統應以多雲基礎建設及早加強數位韌性：

自 2018 年起之美中貿易戰迄今之科技貿易戰，接著新冠變種病毒造成塞港、斷鏈，再到俄烏戰爭加劇能源、通膨等問題，以及近期部分地區緊張的政治關係，各種大環境變化促使我們認清以往可能忽視的明顯風險及應採取的行動措施，也突顯國家政策及數位科技扮演的重要角色，此時若能及早加強「數位韌性」累積籌碼，將更有餘裕面對未來各種政經及資安攻擊事件的衝擊。數位發展部部長唐鳳曾指出,「韌性指的是在任何時候遭受到不利的影響，透過完善機制的即時應變並快速恢復；甚至從被攻擊的經驗中學習、強化自身體質」。就機關而言如果從資訊基礎建設

面為出發點，強化自身資訊服務之備份及備援機制，並輔以雲端服務技術，建構服務不中斷之架構，未來無論面臨預期性或非預期性的系統停機時，都能不中斷的隨時提供資訊服務，使機房不單是資訊機房，而成為本局次世代司法調查資訊中心之永續經營。

隨著雲端技術的進步與成熟，雲端運算的發展與應用，不僅使效率提升與降低成本，更可強化為民服務系統之服務品質與韌性，目前已見許多國家紛紛利用雲端技術的優勢，發展數據、先進的通訊技術及運算技術，加速基礎設施智慧化，由傳統 IT 基礎架構轉向雲端運算。行政院核定前瞻基礎建設計畫-數位建設項下子計畫「強化公部門網路服務與運算雲端基礎設施計畫」(110-114 年)，建置公共服務網路交換中心亦整合臺灣學術網路（TANet)、政府骨幹網路服務（GSN)、臺灣高品質學術研究網路（TWAREN）和中央研究院網路（ASNet)，並推動與民生、財稅、農業、藝文、工程等相關政府服務移轉公有雲，透過公有雲彈性擴充所需資源、確保服務不中斷，提供民眾更佳的數位服務體驗，提升政府網路服務韌性與政府為民服務之雲端服務品質。至此，本局為司法調查機關保存許多機敏資料，如何利用雲端之優勢結合地端的資料儲存以發展雲端應用，已然成為新的課題。本計畫希藉由混合雲架構建置多雲備份及備援機制，達成數位韌性中即便是資料中心機房完全失能時，亦可利用雲端特性立刻恢復重要服務，達成服務不中斷的目標。

近年來量子運算技術的快速進展，也開始對現今使用的加密與解密系統帶來衝擊。過去幾十年來的加密演算法主要是以質因數分解(RSA)與離散對數問題

為安全基礎設計，但量子電腦的出現將可以快速突破這類利用特定演算法設計的加密方法，可預知未來此類密碼將被輕易破解，故近年來密碼研究開始朝向後量子密碼學（Post-quantum cryptography，PQC）進行研究，專門研究能夠抵抗量子電腦可破解的加密演算法，由美國國家標準技術研究院(NIST)號召推動產業界或商用共通標準中。本計畫亦希透過與民間專業密碼研究團隊公私協同合作研究安全的資料加密保存方法，並實踐於前述多雲備份與備援之架構下，使資料保存更安全。

本局全球資訊網系統目前非採雲端架構，所有資料及應用程式(AP)均區域化儲存與運作於本地端，如遭遇例如 DDoS 等網路資安攻擊事件時，官網服務癱瘓或被置換時將明顯缺乏立即回復能力，因此需要在建置完成之安全雲端鏈路及雲端架構下，以業務資訊或個資較不具機敏性及與現有環境相依度不高的服務，或與局內業務關係較低的服務，優先安排雲端化，例如依公開資料、AP、機敏資料順序逐年實施雲端化及雲端備份的機制；反之，則以雲端為冷備份之的標的，建置例如混合雲或多雲的第二資料中心。從而，於符合雲端高可用性及擴充特性下，能夠利用雲端服務及正常維運以滿足資通安全責任的防護要求，以免遭受境外勢力駭侵或於類似俄烏戰爭狀況時服務停擺。

（二）資安戰略規劃應納入零信任網路架構治理範圍及網路犯罪追查系統，併以提升資安維運數位韌性：

NIST 於 2020 年起正式頒布標準文件 NIST SP800-207，將零信任架構分成核心組件與支援組件，

且依第六期「國家資通安全發展方案(110 年至 113 年)」之「善用智慧前瞻科技、主動抵禦潛在威脅」推動策略，藉由發展主動式防禦技術，推動政府機關導入零信任架構，完善政府網際服務網防禦深廣度，本局為資安責任等級 A 級機關，故為優先推動之單位，以此架構規劃組織內部零信任資安架構刻不容緩，而為達成零信任架構有關認證授權、身分及設備鑑別、信任推斷及資安防護等四個關注面向，需落實辦理資通系統等級所需之安全控制措施，經盤點本局現有資訊環境需強化部分有：單一窗口身分驗證及授權、負載平衡及應用程式防火牆、端點軟體管理、端點外接 USB 檔案安全管理、端點 APT 攻擊偵測、網路導流側錄及分析系統、網路流量分析系統、上網閘道資訊安全防護及事件關聯分析監控系統等，需補強上述安全防護，以達成 A 級機關資通系統分級安全控制措施，強化政府整體資安防禦能量。

本局為我國重要犯罪偵查與情報蒐集機構，為能偵辦國家重大犯罪及保障民眾權益，擬定資安戰略時，需賡續訂閱本局輔助使用之軟體服務，持續支援提升本局第一線同仁科技犯罪案事件之偵查能力，以因應科技快速變遷之新興犯罪態樣，方能有效打擊罪犯、突破人工查處之障礙。惟查，現行相關電腦偵辦系統具有以下主要問題：

1. 網路跡證溯源系統之資料範圍、功能、效能均有限：

系統資料源具主流社群軟體如臉書、Twitter、微博等，亦涵蓋 8 萬個資料源，惟因異常帳號常透由另闢新平台、論壇、帳號作為訊息傳遞管道，使此類網路節點逐漸脫離系統涵蓋，導致實務上仍需大量人力搭配系統分析，或以人工新增網路節點標的，才能有

效提升資料涵蓋程度。

近年來境外敵對勢力及有心人士，常利用 AI 假冒、免洗式人頭帳號等科技手法，使司法人員在追溯爭訊的過程中，常需搭配其他科技系統及分析工具結合辦案思維深入剖析，才能阻絕新型態、更隱匿之異常社群行為手法或操作方式。此外境外敵對勢力及有心人士，為避免受我國執法單位查緝，已逐步採用影音、圖文、圖片等型態，作為訊息傳遞主體，該類訊息型態具高容量、分析難度高，迫使司法單位查緝成本亦隨之上升，需不斷擴充原有功能並透由較新資訊科技進行分析，方能有效辨識其內容意涵，突破偵查作為之障礙、有效打擊犯罪。

社群及通訊軟體用戶在目前8萬個網路節點之資料源下，本系統中溯源模組及輿情模組功能，在爬蒐網路資訊速度及效率有一定限制，欲克服此類問題須提升爬蟲程式、爬蟲帳號數量、爬蒐所需伺服器相關硬體效能。

2.暗網犯罪情資搜尋系統查詢成本高昂：

目前公私協力合作之網路威脅情報公司，係由數位取證專家、白帽黑客、網路分析師等多位資訊領域、資安專家組成，具最新資訊安全威脅和攻擊技術知識，並以實務經驗持續抓取、更新暗網數據，確保暗網訊息在發布時輔助本局同仁能快速因應漏洞持續擴散，及時保全暗網資訊，惟囿於授權查詢所費不貲，致查詢數量須嚴格管控，無法支援配發本局外勤同仁使用，因而亟需提升查詢數量及續訂該系統服務，持續支援案件偵辦需求。

3.現場調研側錄封包耗時，需建置移動式設備及雲端中控平台：

隨著網路與資訊設備的普及，使外部公司單位、個人持有電子產品數持續提升，軟體服務供應商亦轉向以雲端方式提供使用者隨時隨地存取其數據和應用程式，使資料不再受限於本地端儲存。本局資安人員蒐獲資安情資、於受駭單位現場針對案關設備進行側錄時，囿於駭客入侵手段多樣，有時不易迅速發現及阻止，需長時間進行封包側錄以收集足夠的證據供掌握入侵範圍及方式，因此需賡續充實資訊安全科技設備，以強化資安調查能力、提升執法效能。

（三）以新興資訊科技促進鑑識分析及系統效能數位升級，強化應用系統數位韌性：

受惠於網路傳輸速度大幅提升、無線通訊普及化與雲端服務基礎建設供應穩定等因素，近年雲端服務應用提供使用者不限地點便捷地存取個人資料，同時亦將重要資料備份於雲端，如何搜扣、保全及鑑識相關雲端資料作為數位證據係現今數位鑑識一大挑戰。本局雖能將自 Google Gmail 及 Drive、Dropbox、Line 及 WeChat 等應用程式所擷取之案關電腦雲端資料保全數位跡證、避免遭受刪除，惟囿於雲端服務軟體版本更版速度快，造成本局與廠商合作開發之雲端資料取證系統需適時調整程式碼，避免面臨無法使用之窘境，亟需不斷維護更新及擴充新服務，以符合本局案件偵辦需求。

本局 111 年數位鑑識案件統計共 967 案(包含六都資安團隊初步檢視報告及局本部資安鑑識實驗室鑑定報告)，鑑識證物計 3,538 件，處理證物容量計 1,185 TB，相較 110 年成長將近 40%，顯見數位鑑識需求持續攀升。基於龐大鑑識分析需求，針對本局每

年招考資訊科學組結訓暨業務相關新進同仁規劃基礎鑑識課程，期能拓展數位鑑識量能至外勤單位辦案人員，以求第一時間在搜索詢問階段納入數位證物鏈環節，透過分析搜扣案關資料，更有效率挖掘出線索及案件突破點。此外，有鑑於電腦犯罪樣態多元，各種駭侵手法、加密及反鑑識機制等技術不斷翻新，鑑識人員唯有不斷精進及學習新穎技術，方能於資安事件發生當下，快速通盤掌握數位跡證，遂有每年安排資安鑑識人員進階訓練之必要性。

（四）**本局針對伺服器與 API 管理及行動調查系統優化，具有效能與功能提升及維持應用系統正常維運之明確需求：**

關於伺服器管理，相關需求及可行方案包括：應導入應用系統使用效能分析軟體，由使用者角度掌握各重要資訊服務之可用性及效能；應收集使用者端、網路（含伺服器）及應用系統等相關效能數據，可關聯至受影響之客戶及交易並透過即時監控儀表板，使資訊單位能快速了解受影響之使用者及業務功能範圍，俾於最短時間內找出問題點進而加以排除，大幅減少 IT 人員查找瓶頸時間及降低營運上的損失；對於應用系統程式效能監控軟體，收集及分析程式執行過程各項效能資訊，應協助開發人員快速發現系統程式碼問題，提高應用系統之軟體品質與服務效能；應建立效能監控數據管理及制定合理的服務水準；應提升系統運維人員在全系統效能監控的效率，無論在部署、設定及監控等方面；及應自動關聯跨系統及跨平台之事件與紀錄檔，並由 AI 自動推薦最有可能的問題根源及影響範圍分析與回播，快速判斷系統效能瓶

頸點，並針對問題自動作成即時分析與回饋。

關於API管理，相關需求及可行方案包括：應導入API管理平台，提供API目錄以檢視API服務規格，協助開發人員快速了解API服務介接方式，減少維護與溝通成本，增加API服務的可視度與再利用率；應提供API Key、HTTP Basic、OAuth、Two-way SSL等多種認證機制，集中管理API服務授權，將安全管控提升至一定的安全水位，並減少在API服務端重複開發相關機制的負擔;應由API服務管理平台進行IP黑/白名單、流量管控、隱碼威脅掃描、敏感性欄位遮罩及檔案型態/容量檢查等多種安全強化機制，提升機關資訊安全防護強度；應透過平台進行API服務使用狀態統計分析，有效掌握各API服務使用率及整體表現，以有效掌握業務動態及資源評估；應監控API服務使用量、反應時間及錯誤率等交易狀態，以及時進行反應而維持各服務具有一定水位之穩定度；及管理平台應提供服務組裝功能，藉由重組既有服務與資料來源，快速依需求提供新的API服務，以減少重複開發的負擔。

關於行動調查系統優化，相關需求及可行方案包括：應改為微服務系統架構，不同的服務可以獨立擴展與部署而不會被其他服務制約，未來後端將全面更換為 Docker 以自動化部署相關服務，並使其更容易維護及測試;應提供單一嫌犯犯罪行為AI分析，透過AI相關技術及結合本局內既有資料庫，針對單一嫌犯找出其可能的犯罪行為模式，例如出入境異常、金流異常及出入港異常等等;及應提供多嫌犯關聯性與集團犯罪行為AI分析，透過AI相關技術及結合調查局內既有資料庫，先找出各嫌犯之間的集團關聯性，例

如出入境相關、金流相關及入出港記錄及三親等、工作同事、軍中同袍、股東及獄友等關係，再給予綜合評分且列出所述評分各屬性之權重分數。

四、社會參與及政策溝通情形

本計畫係以「多雲基礎建設」、「資安戰略規劃」及「數位升級」三項主軸，導入雲端化、AI 及加密與運算等新興技術而建置與維運相關系統，以期達成數位韌性。本局業務因涉及犯罪偵查及國家安全，若內容公開後恐造成犯罪者及敵對勢力得窺調查全貌以規避偵查，嚴重影響國家安全及犯罪偵辦，且所需經費均來自政府預算支出，故並未開放社會參與及政策溝通。

貳、計畫目標

一、目標說明

本計畫希實現「多雲基礎建設」、「資安戰略規劃」、「數位系統升級」目標以達成數位韌性成果，且關於性別目標，除訂定各年度執行策略與分工所需人力性別比例以平衡不同性別之人數比例之外，亦逐年強化與本計畫相關的性別統計與性別分析以落實性別平等法規與政策。內容分述如下：

關於**多雲基礎建設**此一目標，包含能因應戰時之異地分持備份資訊機房、雙活資料中心，以確保機敏資料之可靠與完整性，及公有雲、私有雲之多雲與混合雲架構，以支撐核心業務服務之永續運作；強化機敏資料保護部署，以核心服務對應之資料庫加解密為出發點，施作高強度加密及代碼化措施，確保資料看不到、拿不走、解不開，針對機敏資料保護進行分持備份並持續驗證，與韌性機房基礎設施強化為最後一哩路，打造本局混合雲資訊戰略中心，期透過完整、安全、快速反應之資訊平台，將正確的人，

在正確的時間、正確的地方提取正確之資料，並遵循最高等級資通安全標準，賦予調查人員快速打擊犯罪，指揮階層快速部署調配人力與情資運用的同時，確保機敏資料不外洩且被正確運用；於所建置的雲端安全鏈路環境下，利用資訊系統雲端化來優化服務韌性、品質及使用者網路體驗，藉由雲地混合機制所賦予的雲端備份回復能力，能使本局全球資訊網系統藉由雲端化計算及服務的特性，以及營運持續不中斷之資訊雲服務，提供各項穩定、安全及具有擴充彈性之雲端資訊服務，且讓企業或民眾能快速、安全地獲取相關資訊，進而提升整體網路服務數位創新競爭力，建立符合資通安全責任等級之公務機關業務持續運作可用性，在重要民生關鍵系統及應急時期足以維持基本運作之系統核心功能，並~~能~~採用跨境公有雲雲端儲存服務，將檔案、資料庫加密與分持存儲，提升機關自主操作能力，落實備份、回復與營運持續演練作業及教育訓練。相關內容臚列如下：

（一）**資訊系統永續運作架構**：係因應戰時之雙活資料中心及混合雲服務，更包含：快速災害備援與回復，以保障核心業務持續運作，及機敏資料分持備份與加密含金鑰管理機制，以保障機敏資訊不外洩。

（二）**雙活機房**：達成與優化主、備機房基礎系統與大兩層網路等關鍵架構，及建立高可用性和容錯能力的雙活服務，以確保關鍵業務連續運作。

（三）**分持備份與混合雲戰略**：達成由異地到多副本、多雲之備份存儲位置，及由私有雲跨度至公有雲的混合備份與還原系統。

（四）**全球資訊網系統升級雲端化**：完成雲端移轉、建置

DDoS 攻擊防護、作業系統維運、系統變更開發及教育訓練，使本局網站系統、服務及資料具備數位韌性。

關於**資安戰略規劃**此一目標，包含為求內部組織運作、偵辦、執行案件與勤務過程提取資料之準確性、安全性，並透過對任何資料及應用存取皆永不信任且必須隨時驗證的原則，有必要推動零信任網路(Zero Trust Network)架構及其對應之智能分析與應用服務平台;確保本局案件偵辦現場搜扣數位證據之完整性及有效性、降低證物遭汙染之風險與確保偵審階段之證據證明力;及確保本局於各主流社群平台、暗網上蒐報訊息完整性與即時性，避免有心人士發文後便立即刪除，造成第一線偵辦同仁追查不易之窘境，亦期能降低網路情資蒐報所耗費的時間，實有持續訂閱現行本局輔助使用之科技軟體以賦予調查人員快速打擊犯罪利器。相關內容臚列如下：

(一)**零信任網路架構**：提供混合雲環境之零信任網路服務，包含身分、設備、網路、應用系統、資料及事件治理、雙活機房、分持備份與混合雲服務應用強化等項目，用以全面提升資訊安全與數位韌性，更包含：

1.身分治理：達成未知人員無法使用內部網路。

2.設備治理:達成未知及有安全疑慮設備無法連接內部網路。

3.網路治理：達成未知網路行為無法移動。

4.應用治理：達成未經授權無法存取系統。

5.資料治理：達成未經授權無法存取機敏資料。

6.事件治理：達成事件記錄、告警及自動化處理，提升資訊維運及資安事件可視化及自動化，提高資安團隊的效率，減少漏報和錯誤響應的風險;平台整體運作概念為自動化事件分析、防禦系統協同合作、簡化

資安事件處理、程序化案例管理及產出協助維運決策之報告與指標。

（二）**新世代網路電腦犯罪追查：**確保本局同仁能迅速掌握主流社群媒體散播假訊息、暗網情資等資訊來源，即時執法並建立預警防範機制，以確實保障民眾安全福祉。

關於**數位系統升級**此一目標，係優先導入 AI 等新興資訊科技及網路安全科技，建置並滾動式調整零信任網路架構與智能分析資料存取系統，同時持續整合本局既有如天網、法眼、行動調查等相關指揮系統及影像辨識暨分析調查應用服務平台，強化本局科技辦案能量；及將專用之數位證物保全儲存載體及鑑識軟體初步分析操作訓練推行至本局外勤單位，同時精進資安鑑識實驗室人員之專業職能，以培植第一線人員有關偵辦案件之數位證據保全及分析能力，使關鍵數位證物能即時且完整被擷取，充分發揮本局犯罪調查職掌。相關內容臚列如下：

（一）**新世代數位鑑識：**完善數位證據保全及證物鏈管理，拓展最新鑑識分析技術及方法，厚植資安鑑識人才培育，達成科技輔助辦案之成效，迫使犯罪跡證無所遁形。

（二）**系統效能管理及優化:**建置系統效能監控系統、API 管理平台及擴充本局行動調查暨智慧分析系統，並導入人工智慧技術於 AI 及語音查詢等數位應用，達成系統效能管理及優化目標。

關於性別目標，係訂定各年度執行策略與分工所需人力性別比例，且建立相應資訊系統之使用者、計畫執行

者(例如資安人員、資料庫或機房維運人員及鑑識實驗室操作人員等)及專業訓練講授者與學員明確之性別統計資料及性別友善工作環境與公共空間，以期不同性別者都有機會被看見、培力及照顧。

二、執行與推動

為落實本局服務管理、資訊安全管理與個資管理之標準化政策，由資通安全處統籌架構規劃、人力及經費籌用等事宜。本於「多雲基礎建設」、「資安戰略規劃」、「數位系統升級」目標以達成數位韌性成果，具體執行與推動方向如下：

（一）關於多雲基礎建設此一目標之執行與推動包含：

1. 多雲基礎建設之_雙活機房：

未來指定兩處或多處環境，提供適切之網路及頻寬，使複數機房在部分核心服務做到雙主動式(Active-Active)、主-備式(Active-Standby)及異地備份(Backup)，與異地備援(Replicate)；採取適當的措施保護資料的機密性、完整性和可用性；建立並一併納入零信任網路進行身分認證和存取控制機制，加密敏感資料，建立次世代防火牆、IPS 入侵偵測系統等；及建立大兩層網路（Big Two-Layer Network）架構設計，透過整合兩地核心交換器與閘道器機制，提供高可用性與容錯能力並簡化網路管理。

2. 多雲基礎建設_分持備份與混合雲戰略：

以本局週期性、短期服務、靜態頁面為優先或測試標的，將過往地端運算資源擴充必須歷經冗長的採購、測試及上線過程之相關問題，採用公有雲彈性因應相關需求，免除或部分降低建置及後續維護成本；

及採取混合雲架構建置共構機房，於私有雲擴建保有本局機敏資料管理及落地的優先權，同時擁有隨時可將指定應用連接到各大公有雲的選擇彈性(Azure、AWS、GCP 或各類 IDC 機房)，且加速資料中心和機房數位轉型升級同時，一併確保雲端和地端有一致化的維運、資安與管理機制體驗，對於未來應用與服務創新之需求，以及無法預期的工作負載如天災意外的資源調度，皆可發揮最大化及最迅速的擴充能力。

此外，建置公有雲分持加密、核心系統與資料備份服務時，系統架構可包含「碎形加密儲存保護系統」、「地端碎形節點(DQFS Node)」、「內部使用者入口網站(CMQ)」、「RESTful API 服務接口」及「雲端碎形節點(DQFS Node)」，且技術規格需符合我國「資通安全管理法」不能外洩、不能竄改、不能中斷、機敏性(Confidentiality)、完整性(Integrity)、可用性(Availability)等要求，可普遍使用於資料安全儲存、傳輸及分享之用途，尤其當檔案遭遇受損或駭客入侵風險時，需能自動還原及有效防止資訊外洩。系統架構分述如下：

(1) 碎形加密儲存保護系統：為針對資料儲存與安全設計的系統架構，可以完全杜絕駭客或惡意軟體挾持竊取檔案，將重要機敏資料外洩、散佈，其特色在於將檔案以特殊方式加以碎片化、加密化，藉此達到「隱匿」之效果，主要由地端服務節點、入口站台、API 接口以及雲端服務節點所組成，系統佈建於機關內部虛擬化運算平台，連結內外網網路環境，同時串接雲端服務節點。經過碎形加密後之文件，當駭客入侵資訊系統時，「文件及訊息」之隱匿效果可有效杜絕「駭客」

或「惡意軟體」之挾持，使其竊取、散佈等違法行為無法達成，有效保護機關重要機敏資料。

(2) 地端碎形節點：提供檔案碎形化以及碎片儲存服務，建議基礎建置數量為 3 個節點，可依據資料增長量逐步增加節點數量，以擴大虛擬儲存池的容量需求。

(3) 內部使用者入口網站：提供使用者操作平台，以供文件上傳碎形或下載還原資料以及文件交換群組權限設置。

(4) RESTful API 服務接口：提供呼叫 API 資料碎形與呼叫 API 資料還原功能，以供第三方應用服務層介接。

(5) 雲端碎形節點：於公有雲 IaaS 平台建置檔案碎形化以及碎片儲存服務，可依據資料增長量逐步增加節點數量，以擴大虛擬儲存池的容量需求。

3. 多雲基礎建設_本局全球資訊網系統雲端化：

為達成本局全球資訊網系統升級雲端化，參考國家發展委員會建立之公有雲規範及環境，應了解公有雲相關管理機制、服務及資安規範，評估適合之雲服務供應商、執行相關資訊系統建置、移轉及測試；執行策略應包含雲端化方案分析評估暨架構設計與安全要求、公有雲服務選擇與進駐、雲端部署與上線運作暨系統移轉驗證、運作監控暨維運與安全管理等階段之工作項目內容；依本局現有官網資料及系統特性、作業方式、服務水準、效益成本、導入及建置風險與衝擊評估等進行分析，設計雲端化運作所需之網路、平台主機、資料庫及應用系統等架構，並因應系

統雲端化架構訂定雲端化之安全要求；將通過測試的系統與資料部署於雲端並於通過上線測試後，可正式切換至雲端系統運作；及所訂定資訊系統雲端化移轉及驗測計畫，可包含系統雲端化建置及調整、系統架構測試、系統移轉測試、資料移轉測試、雲端技術特性驗證、壓力測試、資安檢測、資安監控機制整合測試、系統整合測試及系統備份與還原等，並辦理與原單位資料中心之服務介接測試及各項資源調配，確保系統移轉順利。

（二）關於資安戰略規劃此一目標之執行與推動包含：

1. 零信任網路架構_身份治理原則：

同步帳號資訊到所有系統或資料庫，帳號及存取管理包含到整個用戶生命週期；所有應用服務可自動地建立、更新或撤銷使用者的權限，建立基於風險的身份驗證授權機制，依據使用者所在地域、IP、設備屬性、個人屬性、存取歷史習性、時間等自動控制使用者登入認證的方式或直接拒絕存取；整合多因子認證，強化身分驗證，提供如行動自然人憑證(FIDO2 規範)以保護帳號使用安全；及收管特權帳號，使用時應取得授權且強化安全性設定。

2. 零信任網路架構_設備治理原則：

基於信任平台模組(TPM 2.0)設備鑑別與設備健康管理機制，其中 TPM2.0 主要功能包含：用於確立設備的唯一身份，從而實現安全驗證和授權；用於驗證設備啟動過程和軟體升級更新週期的完整性；用於安全存儲加密密鑰，即使設備丟失或被盜也能保護敏感數據；用於安全地存儲密碼，降低密碼被盜或濫用的

風險；及用於確保受信任的軟體在該設備上運行，防止惡意軟件感染。

此外，所有資訊資產軟硬體版本均可線上查閱並提供自動更新功能且做到通過密碼、指紋識別等方式，強制設備使用者進行身份驗證；透過單一平台定期更新所有端點設備上的韌體與 OS(如 Windows update)，以保證設備免受漏洞影響；及透過監控和日誌(Log)記錄功能，追蹤並記錄設備活動，於資安事件發生時查詢歷程變化。

3.零信任網路架構_網路治理原則：

基於端點之網路微分段管理機制，依單位、性質、功能或種類區分不同網段，網段內端點可再進行實體與虛擬化之微分段管理；虛實環境微分段管理機制，可採用軟體定義網路(SDN)，使非法、未經識別之電腦無法連結入侵，並當網路環境內有任何惡意軟體時均無法執行，既便執行也無法橫向移動，故由 SDN 技術控制網路流量且限制對帶有威脅/危險之 IP 地址進行訪問，包含對設備再驗證及相關權限控制，可提高總體安全性；及網路流量流動範圍，包含使用者正在存取受保護資料及採用何種連線方法等，於掌握相依性後，在保護範圍四周就近配置控管機制，建立「微周邊」(Micro perimeter)並使用「分段閘道」的新一代防火牆 (NGFW)來控管，僅允許來自合法使用者和應用程式的已知流量，並運用 Kipling Method 強制執行存取控制，依據人員、內容、時機、位置、原因和方法來定義存取原則。

4.零信任網路架構_應用治理原則：

建立使用者與應用系統之安全連線機制時,透過存取閘道(Access Gateway)負責網路導向與連線，為資通系統(RP)之存取門戶主要且唯一入口，不論來自內或外部網路之存取，必須經由存取閘道並留下紀錄，同時利用如反向代理技術存取全程隱藏內部網路路徑；及應考量實施負載平衡機制以避免效率瓶頸，亦必須實施可有效防止 DDoS 攻擊之機制，同時透過訪問控制如身分驗證和授權驗證等作為，持續監控確認流量是否有異常情形，且為了確保服務之穩定與可靠性，網路與負載平衡機制將同時具備單點失效與防措施，及備份與災難備援計劃，確保總體環境其應用服務維持永續可靠性。

針對 API 的管理、導入 API 管理平台時，藉由管理平台服務組裝功能，重組既有服務與資料來源，快速依需求提供新的 API 服務，減少重複開發的負擔；及將原本散置各伺服器的 API 集中管理，當欲檢視問題時，無須逐台進入檢查，可從管理平台介面進入，快速查找問題，及時排除，確保系統服務的正確性及穩定性。

針對 API 的管理、導入 API 管理平台時，藉由管理平台服務組裝功能，重組既有服務與資料來源，快速依需求提供新的 API 服務，減少重複開發的負擔；及將原本散置各伺服器的 API 集中管理，當欲檢視問題時，無須逐台進入檢查，可從管理平台介面進入，快速查找問題，及時排除，確保系統服務的正確性及穩定性。

針對行動調查系統導入微服務架構時，系統開發

完成後的部署在複雜且龐大的系統架構下，一直是麻煩且容易出錯的過程，其過程需逐一確認對應的伺服器及對應的埠(port)，且還須確保開發環境所建置的 binary 檔案及相關的套件可順利無誤的於正式環境中運行，如能導入 Docker 技術，則上述問題可迎刃而解，降低部署的時間及錯誤的發生率，提高程式開發的效率。

至於建立應用系統與應用系統間之安全連線機制，在各系統之間建立連線前，確保適當的防火牆和網路安全控制已經完備。阻止未授權的活動與訪問，同時只允許必要的連線；各系統之間使用 API 進行溝通前，確保每一段 API 均具有如密鑰、OAuth 授權等，以防止未經授權的訪問；建立所有應用系統活動之監控和日誌管理機制，追蹤和記錄異常活動，同時檢測潛在的安全事件和異常活動，並及時採取應對措施；及定期透過內外部雙向稽核進行系統之間安全連線的風險評估。

5. 零信任網路架構_資料治理原則：

資料治理於資料的生命週期，例如資料取得、傳輸、運用、銷毀等階段，皆無法避免；資料庫應稽核管理，採用如 DAM 技術對使用者及應用程式進行管制措施；機敏資料靜止及傳輸過程均應採用加密、防外洩(DLP)等技術方法，達成機敏資料拿不到、帶不走、看不懂；機敏資料需實施明確的資料分類和標籤(Tag)，並確保合適的安全控制應用於這些資料，如建置單向傳輸加密通道，確保點對點傳輸狀態安全；設立監控機制，追蹤和記錄機敏資料的存取和活動。同

時定期審視和分析監控數據，以檢測潛在的安全事件和異常活動；及行動調查系統資料係案件偵辦過程中機敏資料，所有經由 AI 分析產生的行為模式資料，都將經由資料庫加密技術儲存於資料庫中，且對應的備份檔也將加密處理。

6. 零信任網路架構_事件治理原則：

應包含全部之資訊資產，包含維運類及安全性事件；應建置資安維運管理中心(SOC)，監控機關全部資訊資產安全性事件及網路流量，提供安全性有關之事件告警、分析及響應功能；應建置資訊服務平台，監控機關全部資訊資產維運有關之服務及效能狀況，提供具可用性之有關事件告警及處理功能；及建置事件紀錄儲存系統蒐整各式監控設備及系統稽核來源之各項紀錄，藉由自動化關聯功能研析由單位各系統與網通設備(無論是實體、虛擬或雲端個體)所產生之各項資料流及行為軌跡資料，關聯出可供單位搜尋、監控、分析及視覺化單位的資料以發掘資安潛在威脅及獲得維運決策所需資訊，進一步提供更深入的可見度分析、鑑識以及排解來自檢索所有來源項目的疑難雜症，可讓單位各維運業務同仁更友善協同合作，共用搜尋並新增單位專屬的特定知識，並可自行客製建立維為運分析報告以了解識別趨勢、或去符合法規遵循的規範和舉證，也可以建立互動式儀表板以監控資訊安全的嚴重事件、確保服務層級與其他關鍵效能衡量標準。

此外，資安事件治理平台能使機器資料便於調閱查詢、靈活運用並在組織內帶來更高的維運價值，可

分析由單位的 AP 系統與網通設備所產生之機器資料的大量串流，在數分鐘內即可疑難排解問題並調查重大資安事件，監控單位的點對點骨幹系統可避免服務效能降低或中斷，以即時明確方式獲得維運智慧。資安事件治理平台通常應具備以下重點功能：

(1) 收集及檢索任何機器資料：幾乎能從任何來源、格式及位置，即時收集並檢索任何機器資料，包括套裝軟體和自訂應用套件、應用套件伺服器、網站伺服器、資料庫、網路、虛擬化機器、電信設備、作業系統、感應器等等的資料串流，無需事前「瞭解」資料，只要讓資安事件治理平台備好處理單位的資料，它將立即開始收集並編製索引，而單位即可開始進行搜尋和分析，建立關聯，並針對即時事件作出分析及反應。

(2) 新增知識：資安事件治理平台在搜尋時，自動在單位的機器資料內找到知識，以便單位能馬上開始使用新的資料來源。透過識別、命名以及標記欄位與資料點，單位可以新增更多情境資料與意義至單位的機器資料。從資安事件治理平台應用程式網站內安裝內容、附加元件及應用程式來利用先包裝好的輸入、檢視及搜尋特別使用案例、資料來源及技術。可以參照外部資產管理資料庫、設定管理系統與使用者目錄，豐富易於瞭解的資訊。透過「資料模型」描述機器資料的關係，使資料更具意義並提升可用性。

(3) 監控和警示：轉換搜尋為即時警示以便全天候監控臨界點情況。自動觸發動作，如自動化傳送電子信件、執行補救指令碼或將告警訊息傳送至單

位的系統管理主控台或產生服務中心的重大問題待辦單，並可根據各種臨界、值趨勢狀況及其他複雜模式，如遠端設定檔攻擊、暴力密碼破解攻擊及詐騙案例，設定警示並調整它的細緻度。

(4) 報告及分析：讓每個單位的業務單位與維運單位有能力去分析機器資料。迅速建立進階版圖表及儀表板以便顯示重要的統計趨勢。在無需瞭解搜尋語言的情況下，單位可以由資料模型為基礎，然後使用樞紐分析介面建立報告，並透過簡單的拖放功能來分析複雜的機器資料。從圖表的任何位置深入檢視至原始事件、或其他儀表板、查詢表單、檢視或外部網站。

(5) 儲存與檢視報告：應可整合儲存報告並透過單位的個人電腦或行動裝置來檢視報告，甚至單位可以嵌入報告至第三方的商務應用程式、建立PDF、與重要的相關人員定期或即時分享報告或具有儀表板，讓在單位組織內的每個人都能輕易利用機器資料得到強大見解。

(6) 自訂儀表板與檢視：使用者可利用儀表板編輯器，將多個檢視合併至互動式儀表板，且可透過簡單的拖放介面來編輯儀表板，並使用整合的圖表控制來快速變更圖表類型；儀表板亦可整合多個圖表及單位的即時資料檢視，以符合不同使用者的需求，如管理階層、安全性分析師、商業分析師、稽核人員、開發者及系統管理員。

7. 新世代網路電腦犯罪追查：

關於擴充、開發及維護符合本局資安戰略規劃目標之新世代網路電腦犯罪追查相關案件偵辦系統，應確保現有網路跡證溯源系統、暗網犯罪情資搜尋系統、移動式網路鑑識與網路安全監控設備及雲端中控平台等系統之版本能持續更新、系統漏洞能夠即時修繕，以利依據偵辦案件所需，持續使用及滾動式開發網路犯罪資訊蒐整軟體；關於相關資訊科技設備更新，應新購原有硬體資訊科技設備，提升封包擷錄速度及效率，有助於至受駭單位蒐整網路節點流量。

（三）**關於數位系統升級此一目標之執行與推動包含：**

1. 新世代數位鑑識：

關於資安鑑識設備佈建及效能提升，新購、更新或擴充原有鑑識分析工作站之硬體效能，以提升鑑識效率，並更新實驗室數據資料保存系統；關於新世代鑑識軟體購置暨授權更新，即時確保鑑識軟體保持最新版本且符合實驗室驗證及確效，並依案件所需，蒐羅及開發新式鑑識軟體及工具；關於本局資安鑑識實驗室及六都處檢視操作人員專業訓練，規劃基礎及進階鑑識分析人員專業證照訓練，持續累積本局數位暨資安鑑識應處能力；關於數位證據儲存載體增購及配發，完備第一線人員取得數位證據之成效，配發現場搜扣使用與鑑識分析之儲存載體至本局外勤單位，落實證物管理；及關於開發、擴充及維護符合本局案件偵辦適用之系統，擴充及維護現有雲端資料取證系統，供外勤單位現場搜扣電腦數位證物時使用，且維護實驗室資訊整合

管理平台系統，整合本局數位證物鏈管理並達成進階研析運用。

2. 系統效能管理及優化：

建置、擴充及優化系統效能監控系統、API 管理平台、行動調查暨智慧分析系統，規劃利用新興資訊科技導入 AI 相關應用，且於所擴充行動調查暨智慧分析系統採取負載平衡機制，應用系統端所有閘門都採兩台伺服器互相備援，資料庫除採 SQL always ON 機制兩台互為備援，以達成定期備份且異地備份，確保資料可用性。

三、達成目標之限制

整體計畫所需經費，自 114 年至 117 年預估總金額為新臺幣(下同)5 億 714 萬 7,000 元，在本局預算逐年刪減下，實無法支應本案內軟硬體購置所需，故提出本計畫申請專案經費，以順利完成本局訂定之目標。

四、績效指標、衡量標準及目標值

(一)關於本計畫「多雲基礎建設」此一目標相關之績效指標、衡量標準及目標值，於基於資訊系統永續運作前的提下，需能以雙活機房及分持備份與混合雲等執行策略對資料進行加密、保護及分散儲存，且能逐年完成本局全球資訊網系統雲端化，以落實數位韌性成果。其中，本局目前僅在局本部建置單一資料中心保有全局維運資料，面對預期或非預期的機房服務中斷時，確實缺乏其他可持續運作的方式，故建置雙活機房及分持備份與混合雲戰略，創造多重韌性的服務型態，以達成前述永續運作的目標；至於本局全球資訊網系統升級雲端化，則需逐年依資料及系統應用屬性

完成雲端移轉、建置 DDoS 攻擊防護、作業系統維運、系統變更開發及教育訓練，使本局網站系統、服務及資料具備數位韌性。

（二）關於「資安戰略規劃」此一目標相關績效指標、衡量標準及目標值，由零信任網路架構及新世代網路電腦犯罪追查分述如下：

1. 零信任網路架構係行政院第六期「國家資通安全發展方案」既定政策，包含多面向資訊安全議題的考量，且需就機關既有之資訊架構進行調整補強其不足之處，績效目標包含：

(1) 提高安全性：零信任架構的核心是對所有用戶、設備、應用程序和資料採取嚴格的存取控制，此安全策略下可以減少攻擊者對用戶、設備及應用程序漏洞進行攻擊的風險，從而提高整個系統的安全性。

(2) 減少安全事件：可減少內部和外部的安全事件，即時檢測並應對內部或外部的安全事件，從而減少損失。

(3) 制訂安全性策略：組織內不需要為每個使用者和應用程式配置個別的許可權和安全策略，而可以使用統一的安全策略來簡化管理流程。

(4) 提高效率：零信任架構可以提高使用者和設備的效率，由於安全策略可以自動應用於所有設備和應用程式，因此使用者和設備可以更快地存取所需的資源，從而提高生產力和效率。

2. 新世代網路電腦犯罪追查，其績效目標可由以下方面考量：

(1) 提升系統資料涵蓋程度：具集體性、組織性錯假訊息及情資常需花費大量時間進行資料蒐集、分析及撰寫報告，囿於指派專責人員全天於網路中搜查將耗費大量時間，因此網路跡證溯源系統及其資料涵蓋程度應有助於本局拓展案件來源，可於各大主流社群媒體中協助分析及搜尋可疑帳戶，有效減輕同仁偵查負擔，資安人員之系統使用率作為績效衡量標準，可呈現該系統是否有效且頻繁被使用。

(2) 提升資安情資案源量：於暗網搜尋情資時，苦於使用者身分皆具匿蹤功能及情資分散特性，常需透過人工方式逐步關聯與搜尋，對任務達成時效難免造成影響，因此暗網犯罪情資搜尋系統應有助於本局蒐獲不同的暗網情資來源與態樣，例如公務機關、上市櫃公司或關鍵設施個資外洩、遭勒索軟體等案源蒐報率，有效加速暗網案件發掘及同仁偵查時效，資安人員與外勤處站於協助上級交查及情資運用時之系統使用率作為績效衡量標準，可呈現該系統之暗網資安情資內容是否具有可利用性。

(3) 強化封包側錄與分析能力：以往側錄封包時，苦於駭客啟動遠端操作時間不確定性，長時間側錄受駭單位設備常使市面上其他分析軟體無法相應分析及開啟側錄封包，因此移動式網路鑑識與網路安全監控設備及雲端中控平台應有助於強化資安量能，並提升資安人員於受駭單位現場調研時加速側錄大量封包供分析之能力，可以該移

動式監控設備及平台用於案件偵查分析之使用率(%)作為績效衡量標準。

(4)提升資安情資管理系統優化程度及蒐情明確性：經優化之資安情資管理系統應有助於明確蒐情要項、有效提高同仁所蒐辦情資採用率(核分案件數/蒐報案件總數)。

（三） 關於「數位系統升級」此一目標相關績效指標、衡量標準及目標值，其中，新世代數位鑑識藉由新購、更新或擴充原有鑑識分析軟硬體及雲端資料取證系統，以完善數位證據保全及證物鏈管理，並拓展最新鑑識分析技術及方法，以達成犯罪跡證分析與進階研析運用、厚植資安鑑識人才培育及科技輔助辦案之成效，因此相關績效衡量標準可包含取得資安鑑識相關專業證照人次、每年自雲端資料取證系統可擷取資料之雲端服務增加量；本局系統效能管理及優化則需建置系統效能監控系統、API 管理平台及擴充本局行動調查暨智慧分析系統，並導入 AI 技術於數位應用，以維持系統服務穩定性並契合數位升級戰略與效能管理與優化目標，因此相關績效衡量標準可包含新 API 服務提供率、效能問題報告產出率、AI 分析新功能建置率。

（四）關於性別平等績效指標、衡量標準及目標值，係建立並強化性別統計資料與分析，且以每年主要系統使用、計畫執行者或專業訓練培力講者與學員之性別統計產出率衡量。

（五）各項相關績效指標、衡量標準及目標值

序號	預期績效指標	衡量標準	指標類型	年度績效目標值				現況
				114	115	116	117	
1	提升資訊機房可用性	以新建備援機房1座因應緊急或災難停機之恢復所需工時(小時)	成果型	20	10	8	4	目前僅有局本部資訊機房，24小時內恢復
2	提升資訊服務數位韌性	每年多雲備份及備援節點數增加量(座)	成果型	地端3	雲端1	雲端1	雲端1	目前僅有局本部資訊機房
3	完備統一驗證及授權機制	每年因業務需求使用多因子認證及授權機制累加量(%) 分子：使用人數 分母：需求人數	成果型	20%	40%	60%	100%	0%
4	完備設備管理機制	每年機關可控管設備鑑別與健康管理累加量(%)	成果型	20%	40%	60%	100%	0%
5	完備網路管理機制	機關實施微分段、導流設備、網路流量分析率(%)	成果型	40%	60%	80%	100%	20%
6	完備應用系統安全連線機制	每年使用者以安全機制連線應用系統累加量(%) 分子：使用人數 分母：需求人數	成果型	20%	40%	60%	100%	0%

序號	預期績效指標	衡量標準	指標類型	年度績效目標值				現況
				114	115	116	117	
7	完備資料安全存取及稽核機制	使用者安全存取資料與受稽核率(%)	成果型	20%	30%	40%	50%	10%
8	縮減資安事件預警間及自動化處理人力	資安事件預警平均工時	成果型	1小時	50分	40分	30分	1.5小時
		自動化處理資安事件人力配置(人)	成果型	5	4	3	2	6人
9	完成全球資訊網系統雲端移轉	依資料可公開性及機敏性之雲端化程度(%)	成果型	25%	50%	75%	100%	目前非採雲端架構
10	提升全球資訊網系統資安攻擊抵禦能力	每年接受DDoS攻擊防護率(%)	成果型	100%	100%	100%	100%	目前未具此類防護
11	提升網路跡證溯源系統利用頻度	資安人員之系統使用率(%)	成果型	20%	40%	60%	80%	10%
12	提升暗網資安情資	協助上級交查及外勤處站進行轄區運用情資達成量(件)	成果型	6	6	6	6	5

序號	預期績效指標	衡量標準	指標類型	年度績效目標值				現況
				114	115	116	117	
	內容可利用性							
13	加速大量封包分析能力以強化資安量能	案件偵查分析量(件)	成果型	2	2	2	2	1
14	提升資安情資管理系統優化程度及情蒐明確性	情資採用率(%)，即核分案件數/蒐報案件總數	成果型	72%	74%	76%	78%	70%
15	增進鑑識人員專業能力	取得資安鑑識相關專業證照人次	成果型	30	30	30	30	25
16	精進數位鑑識及現場取證量能	每年自雲端資料取證系統可擷取資料之雲端服務增加量(件)	成果型	2	2	2	2	13
17	完成API管理服務平台建置	新API服務提供率(%)	成果型	100%	100%	100%	100%	目前未建置此平台
18	由系統效能監控平台檢出系統問題成因	效能問題報告產出率(%)	成果型	100%	100%	100%	100%	目前未建置此平台

序號	預期績效指標	衡量標準	指標類型	年度績效目標值				現況
				114	115	116	117	
19	行動調查暨智慧分析系統提供AI分析功能	AI分析新功能建置率(%)	成果型	30%	50%	80%	100%	目前未具備此功能
20	建立並強化性別統計資料與分析	每年主要系統使用、計畫執行者或專業訓練培力講者與學員之性別統計產出率(%)	成果型	100%	100%	100%	100%	0%

參、現行相關政策及方案之檢討

現行相關政策與方案中，例如111年7月行政院第六期「國家資通安全發展方案(110年至113年)」之「善用智慧前瞻科技、主動抵禦潛在威脅」推動策略、111年8月數位發展部數位政府司針對政府重要民生關鍵系統提出雲端備份及回復規劃、國家發展委員會前瞻計畫「強化公部門網路服務與運算雲端基礎設施計畫」之「雲端服務之韌性與品質提升，對外服務利用資訊系統雲端化，優化服務韌性及品質，並建立雲端服務管理制度，提升服務營運效益」、行政院科技部「臺灣資安卓越深耕-先進網路鑑識計畫-網路跡證溯源子計畫(110-113)」之「精進科技與訓練，支援蒐證、反蒐證、通訊監察與電腦犯罪防制等科技監察與蒐證工作，貫徹犯罪查緝及肅貪之政策」推動計畫及法務部113年度目標「推動法務服務智慧轉型，建構數位化科技辦案及創新服務環境，強化資訊安全體系，優化法務行政效能；透過AI協助協助檢察官進行案件之證據辨識」與策略「建構嚴密之安全防護網，

提升安全防護工作，調查、溯源及防堵錯假訊息，並強化偵辦能量，機先防制及發掘境外敵對勢力，或其他非傳統安全危害等狀況,以維社會安定;防制境外敵對勢力之滲透干預，偵處意圖危害國家安全及社會安定之個人或組織，防範高科技營業祕密被竊,以維護國家高科技產業競爭優勢」,已明確揭示：發展並推動政府機關導入零信任網路、完善政府網際服務網防禦深廣度、確保資料可用性、以雲端冷備份優先、後續完善多雲分持及持續進行回復演練、運用科技創新防制新型網路犯罪及發揮鑑識量能等政策。

對照前揭現行政策與方案並檢視本局現況，例如目前營運中之資訊系統建置數量已多達800個虛擬機服務且持續增加中，管理及維運之各類內、外勤應用系統與資料庫伺服器虛擬主機共計300餘台，資料庫容量達100TB，資料筆數超過10億筆，規模較外界資訊（IT）產業之中小型資訊服務公司更為龐大；又如106年起陸續建置六都數位證據檢視分析室，以強化數位證據自主檢視分析能力及辦案量能，迄今約6年之相關鑑識設備軟硬體效能亟需汰舊換新以符合現今鑑識需求,且112年本局已將TAF認證ISO/IEC 17025資安鑑識實驗室測試場域延伸成立高雄資安鑑識實驗室，以加速中南部地區取得鑑定報告時效，亦衍生為新增鑑識人員購置相關軟硬體之需求；且為強化掌控國家安全情勢，因應各項犯罪偵查及數位證據鑑識案件量大幅成長，本局已建置並擬擴充既有資訊架構(如:電子化政府第一階段、第二階段及第三階段)。爰此，基於前揭現行政策、方案、法規與計畫依據為前提，且為因應5G行動網路、雲端服務、大數據資料分析、AI及機器/深度學習等新興科技發展趨勢（如：電子化政府第四階段、第五階段、服務型智慧政府及我國AI科研戰略),本局提出本計畫以持續發展智能、智慧、智動化之軟硬體環境，並

確立「多雲基礎建設」、「資安戰略規劃」及「數位系統升級」三項目標主軸。

基於本計畫「多雲基礎建設」目標，本局將持續完善機房永續營運規劃及多雲戰略高度，給予調查人員快捷、安全、可靠存取應用系統與資料之平台，且逐年完成本局全球資訊網雲端化建置與維運工作，憑藉雲端資安戰略下所建置安全資料鏈路雲端服務可擴充性及可靠性之特性，進行資料分持存儲及制定備份回復及網路攻擊防禦措施，使得網站服務及營運不中斷且能量得以再提升，並強化服務韌性及品質，獲致數位韌性政府成果。

基於本計畫「資安戰略規劃」目標，本局目前建置之資料庫及蒐集網路公開資訊，均可導入自動分析及警示等機制，以深化犯罪調查之能量及國安預警情資之發掘，並將現行資訊與核心業務系統之資安準則拉抬到零信任網路標準，於身份、設備、網路、應用、事件及資料治理均予落實於資安戰略中，同時積極部署網路跡證溯源、情資蒐處及雲端中控架構等網路犯罪追查系統，以全面提升資安維運數位韌性。

基於本計畫「數位系統升級」目標，本局將持續更新數位跡證鑑識所需最新軟硬體設備與版本及取得相關認證，且考量本局業務屬性，案件偵辦有其即時性及持續性，因此相關系統的服務亦不能中斷，如能從監控平台第一時間發生問題並解決問題，可使本局同仁在案件偵辦過程更為順暢，從而加強外界對本局的信任，故於本計畫亦導入系統效能監控平台及 API 管理平台，以期提升本局應用系統穩定度及可用度，且為延續「行動調查暨智慧分析系統」建置計畫，持續擴充系統並活化既有資料，接續導入 AI 技術分析以產生加

值效果，使本局資訊研發技術接軌最新智能化發展。

肆、執行策略及方法

一、主要工作項目及資安防護

（一）對應於本計畫「多雲基礎建設」目標，綜整並臚列主要工作項目如下：

1. 完成異地機房之基礎建設（包含機櫃、電力、空調、線槽配置、網路佈放、監視系統、環控系統、消防系統、發電機）等設施；盤點及評估本局重要基礎設施及系統，採購相對應之軟硬體設備部署於異地機房；評估與選定本局 3 地點部署 3 套地端碎形加密節點並結合加密金鑰管理系統及資料庫或儲存設備連接加密系統，達成資料加密及分散式儲存備份之目標；於異地機房部署相關網路監控及資安防護設備，並租賃網路線路，打通兩地網路連線及對外服務連線，測試資料同步情形及演練單一機房服務中斷時之切換狀況，核心服務於異地機房進行雙活平台建置與測試；及租賃合適之公有雲儲存空間，進行分持備份加密碎片上傳至公有雲進行備份與備份之系統或資料恢復之驗證；強化核心服務於異地機房(含非核心服務遷移至公有雲)之多活平台及其加密含金鑰管理規劃；滾動調整分持備份加密與上傳至跨境公有雲規劃與完整回復至地端之演練模型；及完成多雲資料備份與混合雲戰略系統。

2. 依資料種類與屬性逐年完成本局全球資訊網雲端化，將公開資料、應用程式(AP)及內部交換傳遞之機敏資料逐年於已建置雲端安全鏈路及地端分時或異地備援與傳遞應用，並納入 DDoS 攻擊防護維運，以因應

資安攻擊及數位韌性之戰略需求。

（二）對應於本計畫「資安戰略規劃」目標，綜整並臚列主要工作項目如下：

1. 擇定「行動調查既智慧分析系統」先行導入零信任網路架構，驗證導入工具（包含身分、設備、網路、應用系統、資料、事件管理）；零信任架構擴大驗證範圍，擇定「單一窗口」提供標準化連接用戶帳號及基於風險的身分驗證授權功能，導入「身分管理平台」及「單一簽入管理平台」，及擇定資料中心其他系統及本部使用者提供身分、設備、網路、應用系統、資料、事件管理控管功能；及逐步將全機關使用者、設備及各系統均導入零信任架構。

2. 辦理網路跡證溯源系統更新及資料庫擴充、暗網犯罪情資搜尋系統軟體使用授權及逐步新購六都及資安站所使用之移動式網路鑑識與網路安全監控設備及雲端中控平台。

（三）對應於本計畫「數位系統升級」目標，綜整並臚列主要工作項目如下：

1. 分年新購資安鑑識實驗室基礎設施、數位鑑識主機及外勤人員分析用筆電等設備，辦理相關鑑識軟體授權更新，持續維護鑑識軟體最新授權效期；擴充及維護雲端資料取證系統，維護實驗室資訊整合管理平台，更新實驗室數據資料保存系統等；安排基礎及進階鑑識人員專業訓練，並賡續辦理本局資安鑑識實驗室認證制度延續等工作；增配外勤單位鑑識分析使用之儲存載體，完善數位證據自取得、處理、分析及報告程

序之證物鏈完整性,高度控管本局資安鑑識實驗室及第一線證據檢視分析之流程,嚴守把關產出鑑定及檢視報告之品質。

2. 導入「API 管理平台」、「服務效能監控平台」及「行動調查暨智慧分析系統擴充」,其中「服務效能監控平台」及「行動調查暨智慧分析系統擴充案」,透過機器學習訓練模型建構 AI 分析資料庫,而「行動調查暨智慧分析系統擴充案」將先改為微服務系統架構,並將後端全面更換為 Docker 以簡化系統部署及維護;及持續導入「服務效能監控平台」與「行動調查暨智慧分析系統擴充案」,透過 AI 相關技術以加值資料、持續新增基於 AI 技術之案件偵查分析功能及完成與整合所有開發功能。

(四)資安防護:基於數位發展部提出之零信任部署,本局依此規劃 3 階段資安認證,分別為「身分鑑別」、「設備鑑別」、「信任推斷」,首先以最小信任授權為原則先導入身分鑑別技術,另配合網路之微分段及應用系統之授權管理,達成使用者存取權限的最小化,以確保資料安全,避免未授權之使用者非法存取。另於計畫中亦將建立設備鑑別機制,追蹤並記錄設備活動,以期於第一時間進行異常通報,進行危機處理。信任推斷項目,定期評估並隨時整合本局現有資安設備紀錄,制訂評分規則,以達到自動化阻擋不合規之網路存取,使資安管理人員可準確掌握資安事件並及時查處,避免資安事件繼續擴散,最終確保多雲基礎建設之運作安全,資安戰略規劃之目標能有效達成,數位系統升級後之量能獲得進階提升。

二、各項目概述:

（一）「多雲基礎建設」目標各工作項目說明如下：

1. 建置雙活/多活機房系統：選定本局外勤適當之地理位置及空間，建立與局本部資料中心相當規模之異地機房，機房相關環境建置包含機櫃、電力、空調、線槽配置、網路佈放、監視系統、環控系統、消防系統及發電機等；建置與資料中新相當規模之虛擬環境，選定現有核心應用系統試行資料同步作業，並進行實際演練，演練本地端網路或服務中斷時能否及時切換至備援機房，確保系統、應用程序或服務在發生單個機房故障時仍然能夠保持高可用性和持續運行；擴充與新購負載平衡設備，以因應本局不同實體網段間持續成長之應用服務平均分配內、外網與異地流量之請求，確保所有伺服器工作量能之間平均負載，亦針對 SSL/TLS 工作加速、HTTP、HTTPS 請求內容切換、壓縮等，提供與分散伺服器加密和解密負擔，提高效能；因應未來本局將進行 GSLB(全域負載平衡)提供兩地雙活機房服務，需要負載平衡軟、硬體在多地理位置之間進行流量分配，以確保外部用戶連線至局本部系統得到優化體驗及自動 DNS 切換。

2. 建置公有雲分持加密、核心系統與資料備份服務：建置並實現本局核心資料「分持儲存」備份策略，將資料備份分散存儲在本局不同的設備與位置，包含本、異地及公有雲，轉存雲端前會先將檔案透過加密平台加密並以冗餘的方式進行切割，再分散儲存至公有雲(例如 AWS、GCP 或 AZURE S3 Object Storage 等)；未來任何一份資料毀損皆不影響資料的完整性，取得任何一份資料皆無法讀取完整內容，且至少需要兩份切割後的資料才能完整還原，且加密金鑰亦將一併搭

配外部金鑰管理設備存放，還原前亦須經過密鑰解密，才能讀取正確的資料內容。

3. 建置加密與金鑰管理系統:透過與民間開發之商用加密系統，並混合多種以上的加密方式，將核心業務資料庫加密，搭配存取控管與設立白名單機制進行初步的資料保護。此外，亦針對敏感資料以代碼化及去識別化實施進階保護，令只有驗證過的使用者或系統始可存取資料明文，並確保所有檔案、存儲、虛擬機、資料庫層級的加密均有權責分離的金鑰管理系統，且把最重要的機密(如/PKI 憑證金鑰、私密金鑰)存放於 HSM(Hardware Security Module)亂碼化設備之中，獲得最高層級之保護。

4. 擴增維運系統監控功能:建置並持續擴充軟體定義資料中心的監控與維運平台，藉由持續監控偵測整個虛擬化平台並依照 VMware 的最佳建議來界定基準線確認告警與錯誤;其基準可完全根據本局需求客製化，提供儀表板如同戰情室般呈現，供維運人員直觀分析整體環境概觀，且監控範圍可從虛擬化拓展至實體伺服器、儲存設備、交換器甚至到作業系統與軟體層級(例如 SQL 等)，都能使管理員透過單一平台即可統一監控整個資料中心。

5. 建置及防護本局雲端化全球資訊網系統:進行全球資訊網雲端移轉服務、作業系統維運、系統變更開發及取得雲端化 DDoS 防護授權，並獲取相關雲端化維運技術服務及專業教育訓練，以達成依資料種類與屬性逐年完成本局全球資訊網雲端化及具備 DDoS 攻擊防護維運能力之目標。

（二）「資安戰略規劃」目標各工作項目說明如下：

1. 建置身份管理平台：採用標準化連接方式，同步本局用戶帳號資訊到任何系統或資料庫，存取管理包含到帳號整個生命週期存續與消滅，並根據自定義政策跨越所有應用服務，自動地建立、更新或撤銷使用者權限。

2. 建置單一簽入管理平台：採用基於風險保護的身份驗證授權機制，依據使用者所在地域、IP Address、設備屬性、個人屬性及存取歷史習性、時間等，自動控制使用者登入認證的方式或直接拒絕存取；單一登入整合多因子認證，在強化身分驗證方面，提供如行動自然人憑證(基於 FIDO2 規範)、手機推播驗證、硬體指紋辨識器實體 Token 等標準做法，用以保護帳號使用安全，且使用者因此只需一次性登錄即可在被授權之系統上操作，不需再重複且多次輸入帳號密碼。

3. 擴增資安維運自動響應功能及建置應變機制 EDR (Endpoint Detection and Response)：

持續擴增並導入 SOAR (Security Orchestration, Automation, and Response)資安維運自動響應系統週邊，透過評估既有環境，確認本局現行網路架構、系統和應用程式等逐項分類後，再行整合本局既有資安設備，包括但不限於次世代防火牆、網頁式防火牆、入侵偵測系統、威脅情報工具和其他相關聯之資訊安全產品；同時一併導入流程自動化管理工具，設計和開發日常工作流程自動執行與回應機制，用以提升資安維運的效率，減少處理事件所需的時間，同時降低漏報和錯誤響應的風險，

快速回應網路安全事件，並確保網路安全持續維運。SOAR 平台的主要功能包括：

(1) 跨平台協調：此平台整合不同的資安工具和系統，讓它們之間能夠協同工作，這包括集成 SIEM（Security Information and Event Management）系統、防火牆、入侵檢測系統及終端點安全工具等，使這些工具能夠共享資訊和事件數據，提高整體事件可見性。

(2) 自動化關聯分析：此平台可自動執行預定義的安全操作，例如自動驗證事件、自動調查威脅及自動發送警報通知等。藉由自動化減少手動干預的需求、節省人力成本及加快處理事件速度。

(3) 主動事件響應：此平台可根據事先設定的指引和策略，自動進行響應措施，例如封鎖惡意 IP 地址、隔離受感染的系統及發出警報通知給安全團隊等，有助於迅速控制與處理威脅及防止進一步損害。

(4) 重複案例自動化流程：此平台支援自定義的自動化流程，可以根據不同重複出現的資安事件類型和嚴重程度，設計和定製不同的處理流程，使得安全團隊能夠更加靈活地應對各種不同的威脅和事件。

EDR 主要目的為偵測端點系統上異常活動，以期能及早發現駭客活動跡象，以降低後續可能引發之資安風險，而資通安全管理法法遵要求所有 A、B 級機關須在 112 年 8 月 23 日前完成導入 EDR；端點事件紀錄及觸發事件透過端點代理程式回報，端點伺

服器中控透過 signature 及 IOC 等情資觸發 SIEM 事件，結合觸發高風險 SIEM 事件後，傳至 Arcsight SOC 中心由資安專員負責處理回報，若能結合 SOC 及 SOAR 零信任架構機制，可將異常端點隔離獨立網路，並藉由 SOC 中心發布可疑 signature 或 IOC 等情資，針對全局端點掃描並分析是否遭到駭侵。

4. 建置與擴增資產管理系統、建置端點偵測及資通安全弱點通報機制及擴增軟體更新系統：

(1) 建置與擴增資產管理系統，能助於組織有效地追蹤、監控和管理其所有資產，包括設備、軟體、硬體、文檔與其他價值資產，並結合弱點管理掌握整體風險情勢，協助機關落實資通安全管理法之資產盤點與風險評估應辦事項。

(2) 建置資通安全弱點通報系統 VANS (Vulnerability Analysis and Notice System)，結合資訊資產管理與弱點管理，以供掌握整體風險情勢，而資通安全管理法法遵要求所有 A、B 級機關須在 112 年 8 月 23 日前完成導入 VANS；本局透過 Forescout 蒐集端點資產資訊及弱點資訊，搭配 VANS Server 產生報表上傳至 VANS 平台;以往端點稽核需耗費人力點擊程式也由 Forescout 取代，大幅減輕資訊人員負擔，並能時刻保持端點之合規性，若結合資通設備(switch)或 EDR(carbon black)自動化隔離未合規及異常端點，可保護網路中其他正常電腦及主機；Forescout 亦可設置外接裝置白名單，達到 USB 控管觸發 NAC 規則進行設備阻斷機制。

(3) 擴增軟體更新系統：擴增目前本局既有或新建置自動化軟體更新(patch hot fix 系統)，透過大量部署掃描端點設備，檢測已安裝軟體漏洞及缺陷以修補問題而提高系統安全性。其中，亦包含自動軟體更新、快速即時反應(關鍵性軟體更新釋出時，立即識別受影響的系統並啟動更新過程)、排程與優先等級設定及中央控制與管理，且搭配報告與分析系統以查看不同層面的更新狀態，包括設備已更新、未更新及更新成功率等。

5. 擴增資安誘捕防禦系統：建置及模擬擬真之內部環境，監控潛在的駭客或惡意軟體攻擊，以收集關於攻擊者的資訊、潛在威脅及攻擊模式的相關資料；資安誘捕系統主要是用於保護實際的資訊環境免受攻擊，同時提供對攻擊活動寶貴的資料收集，而攻擊者行為的資訊、攻擊次數、攻擊模式、使用工具及攻擊者的身份追蹤等資訊，有助於分析攻擊趨勢、改進安全策略及提高安全意識。

6. 新世代網路電腦犯罪追查軟體授權及鑑識與監控系統設備更新：賡續購置、更新現有網路跡證溯源系統、暗網犯罪情資搜尋系統軟體授權，並就網路鑑識與網路安全監控系統設備逐步更新外勤處站使用之硬體設備，提升系統處理效能確保於受駭單位進行側錄封包時，系統分析及處理之時效，俾利本局同仁於社群媒體及暗網平台等來源發掘更多案件資訊。

(三)「數位系統升級」目標各工作項目說明如下：

1. 資安鑑識設備佈建及效能提升：規劃局本部、高雄兩地資安鑑識實驗室及六都處證據檢視分析室之硬體

效能提升(含汰舊換新),以加速處理大容量鑑識檔案之效率。

2. 新世代鑑識軟體購置暨授權更新:持續更新現有數位鑑識相關軟體授權,並因應新型態犯罪類型可能衍生之分析資料,購置或開發相對應軟體工具,俾利挖掘更多案關跡證。

3. 資安鑑識實驗室及六都處檢視操作人員專業訓練:依人員背景及執行業務內容規劃資安鑑識相關證照訓練,分為基礎及進階兩部分。基礎訓練包含 TAF ISO/IEC 17025 實驗室認證規範、Magnet AXIOM Examinations、Cellebrite Certified Operator 及 Cellebrite Certified Physical Analyst 等相關課程;進階訓練包含 Magnet AXIOM Advanced Computer Forensics、Cellebrite Advanced Smartphone Analysis、EC-Council Computer Hacking Forensic Investigator 及 Certified Ethical Hacker 等相關課程。

4. 數位證據儲存載體增購及配發:依外勤單位案件需求量,每年滾動式調整配發外勤單位執行數位鑑識分析之儲存載體數量,以確保數位證據擷取、處理及檢視分析過程之有效性及不受汙染。

5. 維護實驗室資訊整合管理平台系統,強化實驗室管理制度並達成進階研析目標;擴充及維護本局搜索現場用之雲端資料取證系統,以即時保全案關數位證物不受刪除。

6. 建置 API 管理平台:可透過平台進行 API 服務使用狀

態統計分析，以有效掌握各 API 服務使用率、整體表現、業務動態及資源評估；藉由管理平台，可從已納管的 API 中快速開發新的 API 服務，達到資源共享及敏捷開發目標。

7. 建置系統效能監控平台：提升系統運維人員在全系統效能監控效率及部署、設定與監控管理；自動關連跨系統及跨平台的事件及記錄檔，並由 AI 自動推薦最有可能的問題根源分析、影響範圍分析與回播，快速判斷系統效能瓶頸點，並針對問題自動即時分析與回饋。

8. 擴充行動調查暨智慧分析系統：目前行動調查系統的後端服務建構在 IIS 的網站上，部署過程繁瑣，且管理上不易符合 ISMS 的規範，例如如何確保 GIT 程式碼與正式機 Server 的程式碼一致，透過 hash 碼檢查程式碼一致性顯然不可行，是以後端將全面更換為 Docker 自動化部署後端服務以期易於維護與測試；全面檢視行動調查系統資料來源是否為局外的其他政府機關系統，規劃更為完善的資料串接機制及網頁爬蟲機制，以獲取局內所需的資料，並結合 AI 技術協助分析嫌犯個人基本資訊及與犯罪集團內成員關係等。

三、分期（年）執行策略

（一）114 年度執行項目與策略：

執行項目	執行策略
■ 多雲基礎建設_異地機房建置、分持備份與混合雲戰略、本局全球資訊網系統升級雲端化： 1.選定適合地點之異地機房空間。 2.建置機房之基礎建設，包含機櫃、空調、線槽配置、網路佈放等設施。 3.於本局選定 3 地點部署 3 套地端碎形加密節點儲存備份系統。 4.於碎形加密器之前端再增加加密金鑰管理系統，以混合式加密方式強化資料保密措施。 5.測試與資料庫或儲存設備連接之加、解密狀況，評估效能。 6.建置DDoS攻擊防護及雲端移轉。	1.辦理採購作業如下： (1)異地機房基礎建設 1 式。 (2)維運系統監控 1 式。 (3)無人機房 KVM 管理系統 1 式。 (4)碎型加密設備地端節點建置 1 式。 (5)加密與金鑰管理系統 1 式。 (6)本局全球資訊網系統公開資料雲端移轉、DDoS 攻擊防護授權、作業系統維運、維運技術服務、專業教育訓練每年 6 人次。
■ 資安戰略規劃_零信任網路架構、新世代網路電腦犯罪追查： 1.更新網路設備為可支援802.1X協定及網路為分段功能之設備。 2.整合AD環境之帳號管理系統及提供多因子身分驗證管理功能。 3.與本局單一窗口之應用系統「行動調查既智慧分析系統」介接以驗證身分識別功能。 4.建置與擴充網路跡證溯源系統、網路鑑識與網路安全監控系統、暗網犯罪情資搜尋系統及資安情資管理系統。	1.辦理採購作業如下： (1)零信任架構網路設備 1 式。 (2)身份及設備存取驗證管理系統 1 式。 (3)身份認證指紋碟 1 式。 (4)SIEM 整合 SOAR 視覺化系統 1 式。 (5)資安誘捕防禦系統 1 式。 (6)網路跡證溯源系統軟體使用授權暨硬體維護 1 式。 (7)網路鑑識與網路安全監控系統擴充 1 批。 (8)暗網犯罪情資搜尋系統軟體使用授權 1 式。 (9)資安情資管理系統(E 平台)。

執行項目	執行策略
■ 數位系統升級_新世代數位鑑識、系統效能管理與優化： 1.採購各式數位鑑識軟硬體、數位證據儲存載體、實驗室資訊整合管理平台擴充暨維護、雲端資料取證系統擴充暨維護、採購實驗室數據資料保存系統、採購並安排鑑識分析相關人員專業訓練等。 2.建置 API 管理平台之軟體、伺服器效能監控平台之軟體、行動調查系統擴充案所需軟體及硬體。	1.辦理採購作業如下： (1)各式數位鑑識軟體授權更新 1 批。 (2)數位證據儲存載體 1 批。 (3)實驗室資訊整合管理平台擴充暨維護 1 式。 (4)雲端資料取證系統擴充暨維護 1 式。 (5)實驗室數據資料保存系統 1 式。 (6)採購並安排鑑識分析相關人員專業訓練：基礎鑑識人員訓練 20 人次、進階分析操作人員訓練 10 人次。 (7)採購 API 管理平台軟體 1 套。 (8)採購系統效能監控平台 1 套。 (9)搭載 GPU 伺服器 2 台。 (10)微服務架構開發，完成率 30%。

(二) 115 年度執行項目與策略：

執行項目	執行策略
■ 多雲基礎建設_異地機房建置、分持備份與混合雲戰略、本局全球資訊網系統升級雲端化： 1.盤點及評估本局重要系統，採購與本地相等及對應之軟、硬體設備部署於異地機房。 2.部署相關網路監控及資安防護設備。 3.租賃網路線路，打通2地網路連線及對外服務連線。 4.測試資料同步情形及演練單一機房服務中斷時之切換狀況。 5.評估及租賃合適之公有雲，規劃公有雲 S3 雲端空間服務環境佈建。 6.進行分持備份加密碎片上傳至公有雲備份與系統恢復之驗證。 7.建置地端碎形服務節點與雲端空間之備份與系統還原機制系統架構。	1.辦理採購作業如下： (1)維運系統監控1式。 (2)異地機房軟、硬體設備1式。 (3)網路線路租賃1式。 (4)公有雲分持系統1式。 (5)公有雲租賃1式。 (6)地端備份及公有雲介接建置1式。 (7)混合雲加密安全系統維護及客製化功能增設1式。 (8)AP 雲端移轉。 (9)DDoS 攻擊防護授權。 (10)作業系統維運。 (11)維運技術服務。 (12)專業教育訓練每年6人次。
■ 資安戰略規劃_零信任網路架構、新世代網路電腦犯罪追查： 1.擴大驗證範圍，擇定「單一窗口」提供標準化連接用戶帳號及基於風險的身分驗證及授權功能。 2.導入身分管理系統與單一簽入管理平台進行整合，將身份驗證及應用系統授權整合為一。 3.建置與擴充網路跡證溯源系統、網路鑑識與網路安全監控系統、暗網犯罪情資搜尋系統及資安情資管理系統。	1.辦理採購作業如下： (1)SIEM 整合 SOAR 視覺化系統1式。 (2)完整端點安全防護系統1式。 (3)網路跡證溯源系統軟體使用授權暨硬體維護1式。 (4)網路鑑識與網路安全監控系統擴充1批。 (5)暗網犯罪情資搜尋系統軟體使用授權1式。 (6)資安情資管理系統(E平台)。

執行項目	執行策略
■ 數位系統升級_新世代數位鑑識、系統效能管理與優化： 1.採購各式數位鑑識軟硬體、數位證據儲存載體、實驗室資訊整合管理平台擴充暨維護、雲端資料取證系統擴充暨維護、採購實驗室數據資料保存系統、採購並安排鑑識分析相關人員專業訓練等。 2.建置伺服器效能監控平台之軟體。 3.建置行動調查系統擴充案所需軟體。	1.辦理採購作業如下： (1)各式數位鑑識軟體授權更新1批。 (2)數位證據儲存載體1批。 (3)實驗室資訊整合管理平台擴充暨維護1式。 (4)雲端資料取證系統擴充暨維護 1式。 (5)實驗室數據資料保存系統1式。 (6)採購並安排鑑識分析相關人員專業訓練：基礎鑑識人員訓練20人次、進階分析操作人員訓練10人次。 (7)採購系統效能監控平台1套。 (8)微服務架構開發，完成率60%。 (9)AI分析功能開發，完成率30%。

(三)116年度執行項目與策略：

執行項目	執行策略
■ 多雲基礎建設_異地機房建置、分持備份與混合雲戰略、本局全球資訊網系統升級雲端化： 1.持續維運異地機房之設備及環境監控。 2.規劃多雲運算服務環境佈建。 3.建置雲端碎形服務節點。 4.建置外部使用者入口網站服務。 5.完善多雲平台備援與系統還原機制。 6.建置 DDoS 攻擊防護及雲端移轉。	1.辦理採購作業如下： (1)維運系統監控1式。 (2)網路線路租賃1式。 (3)公有雲分持系統1式。 (4)公有雲租賃1式。 (5)地端備份及公有雲介接建置1式。 (6)混合雲加密安全系統維護及客製化功能增設1式。 (7)非機敏資料雲端移轉。 (8)DDoS攻擊防護授權。 (9)作業系統維運。 (10)維運技術服務。 (11)專業教育訓練每年6人次。

執行項目	執行策略
■ 資安戰略規劃_零信任網路架構、新世代網路電腦犯罪追查： 1.擴大驗證範圍，擇定資料中心及本部提供身分、設備、網路、應用系統、資料、事件管理控管功能。 2.建置與擴充網路跡證溯源系統、網路鑑識與網路安全監控系統、暗網犯罪情資搜尋系統及資安情資管理系統。	1.辦理採購作業如下： (1)資產管理系統建置1式。 (2)SIEM整合SOAR視覺化系統1式。 (3)網路跡證溯源系統軟體使用授權暨硬體維護1式。 (4)網路鑑識與網路安全監控系統擴充1批。 (5)暗網犯罪情資搜尋系統軟體使用授權1式。 (6)資安情資管理系統(E平台)。
■ 數位系統升級_新世代數位鑑識、系統效能管理與優化： 1.採購各式數位鑑識軟硬體、數位證據儲存載體、實驗室資訊整合管理平台擴充暨維護、雲端資料取證系統擴充暨維護、採購高階鑑識工作站、採購實驗室數據資料保存系統、採購並安排鑑識分析相關人員專業訓練等。 2.建置伺服器效能監控平台之軟體。 3.建置行動調查系統擴充案所需軟體。	1.辦理採購作業如下： (1)各式數位鑑識軟體授權更新1批。 (2)數位證據儲存載體1批。 (3)實驗室資訊整合管理平台擴充暨維護1式。 (4)雲端資料取證系統擴充暨維護 1式。 (5)高階鑑識工作站9台。 (6)實驗室數據資料保存系統1式。 (7)採購並安排鑑識分析相關人員專業訓練：基礎鑑識人員訓練20人次、進階分析操作人員訓練10人次。 (8)採購系統效能監控平台1套。 (9)微服務架構開發，完成率90%。 (10)AI分析功能開發，完成率60%。

（四）117 年度執行項目與策略：

執行項目	執行策略
■ 多雲基礎建設_異地機房建置、分持備份與混合雲戰略、本局全球資訊網系統升級雲端化： 1.持續維運異地機房之設備及環境監控。 2.系統更新及維護，滾動式調整系統效能及架構。 3.依據實際業務規模增長，擴增碎形服務節點與儲存空間。 4.強化服務節點偵測、資料同步與自動資料數據恢復等數位韌性架構機制。 5.建置 DDoS 攻擊防護及雲端移轉。	1.辦理採購作業如下： (1)維運系統監控 1 式。 (2)網路線路租賃 1 式。 (3)公有雲租賃 1 式。 (4)地端備份及公有雲介接建置 1 式。 (5)混合雲加密安全系統維護及客製化功能增設 1 式。 (6)非機敏資料雲端移轉。 (7)DDoS 攻擊防護授權。 (8)作業系統維運。 (9)維運技術服務。 (10)專業教育訓練每年 6 人次。
■ 資安戰略規劃_零信任網路架構、新世代網路電腦犯罪追查： 1.全機關使用者、設備、應用系統均導入零信任架構。 2.建置與擴充網路跡證溯源系統、網路鑑識與網路安全監控系統、暗網犯罪情資搜尋系統及資安情資管理系統。	1.辦理採購作業如下： (1)SIEM 整合 SOAR 視覺化系統 1 式。 (2)網路跡證溯源系統軟體使用授權暨硬體維護 1 式。 (3)網路鑑識與網路安全監控系統擴充 1 批。 (4)暗網犯罪情資搜尋系統軟體使用授權 1 式。 (5)資安情資管理系統(E 平台)。
■ 數位系統升級_新世代數位鑑識、系統效能管理與優化： 1.採購各式數位鑑識軟硬體、數位證據儲存載體、實驗室資訊整合管理平台擴充暨維護、雲端資料取證系統擴充暨維護、採購高階鑑識工作站、採購數位證據資料擷取工具、採購並安排鑑識分析相關人員專業訓練等。 2.建置伺服器效能監控平台之軟體。 3.建置行動調查系統擴充案所需軟體。	1.辦理採購作業如下： (1)各式數位鑑識軟體授權更新 1 批。 (2)數位證據儲存載體 1 批。 (3)實驗室資訊整合管理平台擴充暨維護 1 式。 (4)雲端資料取證系統擴充暨維護 1 式。 (5)高階鑑識工作站 9 台。 (6)數位證據資料擷取工具等 1 批。 (7)採購並安排鑑識分析相關人員專業訓練：基礎鑑識人員訓練 20 人次、進階分析操作人員訓練 10 人次。 (8)採購系統效能監控平台 1 套。 (9)微服務架構開發，完成率 100%。 (10)AI 分析功能開發，完成率 100%。

四、執行步驟（方法）與分工

執行年度	執行步驟（方法）	分工
114	1.指定權責人員蒐集數位韌性及零信任網路架構之相關基礎軟、硬體設施，並蒐集三大平台之基礎硬體、行動調查系統擴充軟體規劃與設計及相關網路架構設計，進行規劃與設計，並擇定共同合作開發之廠商。 2.擬訂採購計畫。 3.辦理設備招標採購作業。 4.辦理驗收及教育訓練，包含辦理鑑識專業人員相關證照教育訓練。 5.建立各平台管理員管理流程標準機制及相關資安規範。 6.確保達成績效指標及目標值要求之作為。 7.執行細節參閱肆、三、分期（年）執行策略。	一、因事涉多項軟硬體採購及不同領域，故分工情形將以業管單位運用現有人力辦理。 二、部分技術研究開發將與國內廠商共同合作開發。
115	1.測試異地機房資料同步情形及演練單一機房服務中斷時之切換狀況。 2.進行分持備份加密碎片上傳至公有雲備份與系統恢復之驗證。 3.導入身分管理系統與單一簽入管理平台進行整合，將身份驗證及應用系統授權合一。 4.其餘同上。	同上。
116	1.持續維運異地機房之設備及環境監控。 2.完善多雲平台備援與系統還原機制。 3.擇定資料中心及本部提供身分、設備、網路、應用系統、資料、事件管理控管功能。	同上。

	4.其餘同上。	
117	1.持續維運異地機房之設備及環境監控。 2.強化服務節點偵測、資料同步與自動資料數據恢復等數位韌性架構機制。 3.全機關導使用者、設備、應用系統均導入零信任架構。 4.其餘同上。	同上。

伍、期程與資源需求

一、計畫期程：本計畫整體期程為114年至117年。

二、所需資源說明

基於本局科技辦案發展與支援外勤科技蒐證需求前提，本計畫所需資源包括人力執行面與經費需求面二部分，分述如次：

(一)人力資源

1. 性別目標：以「強化與本計畫相關的性別統計與性別分析」及「建構性別友善工作環境與公共空間」為主，且本計畫各年度執行策略與分工所需人力，以運用本局各業管單位內員額調派共同辦理及資通安全處為主要人力，目前本處同仁參與及執行者男女性別比為1：1，單一性別未低於三分之一，故可視實際需求於適當空間建置相關設施諸如女性夜間人員備勤室或男、女浴廁等。有關執行本計畫各年度核心工作主要決策與規劃(執行)者性別比例詳如下表。

各年度 男女人數 項 目	114 年度		115 年度		116 年度		117 年度	
	男	女	男	女	男	女	男	女
決策者	4	2	4	2	4	2	4	2
規劃（執行）者	11	13	11	13	11	13	11	13
小計人數	30		30		30		30	
女性比例	50%		50%		50%		50%	

2. 績效指標、衡量標準及目標值：本計畫係整合「多雲基礎建設」、「全球資訊網升級雲端化」、「零信任網路架構」、「新世代網路電腦犯罪追查」、「新世代數位鑑識」及「系統效能管理及優化」之整合型計畫，相關績效指標如前揭「貳、四、(五) 各項相關績效指標、衡量標準及目標值」所述，且其中涉及性別目標所需人力資源者，除基於性別平等政策與精神鼓勵不同性別參與本計畫之研擬規劃與執行推動(本計畫女性參與比例已達二分之一，得以確保任一性別參與比例皆不低於三分之一之要求)之外，亦以「建立並強化性別統計資料與分析」、「每年主要系統使用、計畫執行者或專業訓練培力講者與學員之性別統計產出率(%)」作為預期績效指標及相應之衡量標準，具體之性別統計項目及內容依個案決定，例示如下表。

年度 男女人數/百分比 性別統計 項目	114 年度						115 年度						116 年度						117 年度					
	男			女			男			女			男			女			男			女		
	中高齡	教育程度	使用區域	中高齡	教育程度	使用區域	中高齡	教育程度	使用區域	中高齡	教育程度		使用區域	中高齡	教育程度	使用區域	中高齡	教育程度	使用區域	中高齡	教育程度	使用區域	中高齡	教育程度	使用區域
多因子認證使用者																								
以安全機制連線應用系統使用者																								

使用者安全存取資料使用者																						
網路跡證溯源系統使用者																						
暗網犯罪情資搜尋系統使用者																						
資安情資管理系統使用者																						
取得資安專業證照者																						
取得鑑識專業證照者																						
鑑識實驗室人員																						
鑑識分析相關人員專業訓練講者																						
鑑識分析相關人員專業訓練學員																						
行動調查暨智慧分析系統使用者																						

(二)經費資源

本計畫預定期程為114年至117年，4個年度執行所需經費共計5億714萬7,000元，所編製經費需求表如附表一，其中，依本計畫三項目標對應之辦理項目，分別為依「多雲基礎建設」目標辦理「建置雙活/多活機房系統」、「建置公有雲分持加密、核心系統與資料備份服務」、「建置加密與金鑰管理系統」、「擴增維運系統監控功能」及「建置及防護本局雲端化全球資訊網系統」等項目，依「資安戰略規劃」目標辦理「建置身份管理平台」、「建置單一簽入管理平台」、「擴增資安維運自動響應功能及建置端點偵測及應變機制」、「建置與擴增資產管理系統、建置資通安全弱點通報機制及擴增軟體更新系統」、「擴增資安誘捕防禦系統」及「新世代網路電腦犯罪追查軟體授權及鑑識與監控系統設備更新」等項目，依「數位系統升級」目標辦理「資安鑑識設備佈建

及效能提升」、「新世代鑑識軟體購置暨授權更新」、「資安鑑識實驗室及六都處檢視操作人員專業訓練」、「數位證據儲存載體增購及配發」、「維護實驗室資訊整合管理平台系統」、「建置 API 管理平台」、「建置系統效能監控平台」及「擴充行動調查暨智慧分析系統」等項目，分年所需經費為 114 年度 1 億 4,606 萬元、115 年度 1 億 6,865 萬 7,000 元，116 年度 9,630 萬 2,000 元及 117 年度 9,612 萬 8,000 元，且各細項、總經費、經常門及廠商報價單編號亦詳如附表一，廠商報價單、產品規格或服務內容則詳如附件。

三、經費來源及計算基準

（一）經費來源：中央政府總預算。

（二）計算基準：廠商報價或自政府電子採購網公開取得類同設備或服務之得標價、或臺灣銀行共同供應契約價計算。

四、經費需求（含分年經費）及與中程歲出概算額度配合情形

年度	類別	年度所需經費（單位：千元）	中程歲出概算額度配合情形
114	資本門	86,642	本計畫所列設備係因應本局任務需要，配合現階段工作重點覈實編列，如納入經常性預算於調查局主管預算額度內逐年汰購，在整體預算資源有限下勢將受到排擠，確實無力支應核心業務所需建置之設備經費，恐將無法依本局所提計畫規劃時程，支應本局因應維護國家安全情勢發展所需建
	經常門	59,418	
115	資本門	101,529	
	經常門	67,128	
116	資本門	22,647	
	經常門	73,655	

117	資本門	25,335	置之機密性、高科技化設備及環境技術。 本局執行國家安全維護工作，在面對愈來愈快速的全球化及資訊化時代，有關科技辦案及偵查蒐證等設備卻無法與時俱進，適時針對各類犯罪態樣反制精進，對國家安全所造成之負面影響將無法彌補。 **本計畫建請專案匡列預算額度。**
	經常門	70,793	
	合計	**507,147**	

陸、預期效果及影響

達成「多雲基礎建設、資安戰略規劃、數位系統升級」目標，預期可具數位韌性成果。就「多雲基礎建設」目標預期效果及影響而言，其可建構本局多元異質的數位韌性，究其原因在於所建置雙活機房架構具有高可用性，能確保系統、應用程序或服務在發生單個機房故障時仍然能夠保持和持續運行；具有故障容忍性，即使一個機房中的硬體或軟體出現故障，系統仍然可繼續運行;具有地理冗餘性,機房位於不同的地理位置，可不受到相同自然災害或人為事故的影響；其建置時有考量容量和負載平衡，更好地分散工作負載、減輕單個機房的壓力，且能減少維護對服務的影響，在一個機房需要進行維護時，另一個機房可以接管工作，實現零停機維護；且具備災難恢復能力，如遭受重大故障或災難，可以使用另一個機房來幫助組織快速恢復營運。此外，本局全球資訊網系統完成雲端化升級及具備防禦 DDoS 攻擊能力後，藉由升級雲端架構強化公部門網路服務與運算能力，於網站服務及營運不中斷且能量得以再提升前提下，亦有助於強化服務韌性及品質，並提升對外或為民服務營運效益。

就「資安戰略規劃」目標預期效果及影響而言，將零信任網路架構治理及網路犯罪追查系統納入資安戰略，預期可益於提升資安維運數位韌性。其中，所建構零信任網路架構可達成未知網路行為無法移動及未知人員無法直接使用內部網路；透過多因子認證身份技術，使未經授權人員無法存取系統、機敏資料及內部資源；能有效管理和監控各種設備，達成未知及有安全疑慮設備無法連接內部網路；能有效管理和控制應用程式的開發、部署、使用和維護，確保應用程式在安全、可靠、合規和高效的環境中運行；能達成零信任架構中事件記錄、告警及自動化處理，減少人力監控及處理時效；對機敏資料進行保護，確保資料正確性及不被竄改。此外，所建置或擴充之新世代網路電腦犯罪追查各系統，可依司法人員調查所需，與國內軟體廠商客製化開發，提供本局同仁針對社群媒體中錯假訊息客製化的搜尋服務。在與本局規劃、開發過程中，公私協力交流，進而開發市面上未具之行為數據分析系統，有助提升我國相關產業。

就「數位系統升級」目標預期效果及影響而言，導入新興資訊科技能促進鑑識分析及局內系統效能數位升級、強化應用系統數位韌性。其中，新世代數位鑑識藉由優化及採購數位鑑識軟硬體進行案關數位跡證鑑識、開發及維護相關系統及進行專業人才培育，能夠精進鑑驗品質、提供偵審司法機關正確的鑑定報告、提高鑑驗之公信力，使犯罪者無所遁形，落實保障人權維護、司法正義精神及保障人民福祉；系統效能管理及優化藉由升級既有應用及行動調查等系統，且導入人工智慧技術應用，能有效提高系統效能、穩定維運及提供與時俱進之新查詢方式，優化使用者經驗，亦有助於強化各應用系統數位韌性。

柒、財務計畫

本計畫目的係執行「多雲基礎建設、資安戰略規劃、數位系統升級」目標、實踐「資安即國安」戰略並取得數位韌性成果，並以建置「異地機房」、「分持備份與混合雲戰略平台」、「零信任網路架構」、完成「本局全球資訊網系統雲端移轉及DDoS攻擊防護」及建置、擴充、維護及實施「網路跡證溯源、網路鑑識與網路安全監控、暗網犯罪情資搜尋、雲端資料取證、實驗室數據資料保存、行動調查暨智慧分析、系統效能監控等系統」與「移動式網路鑑識與網路安全監控設備及雲端中控、實驗室資訊整合管理、API管理等平台」為主要執行策略與方法，因係屬社會發展類型計畫，並無涉及民間財務參與投入之情形，所需經費均來自中央政府總預算支出。

捌、附則

一、替選方案之分析及評估：無。

二、風險管理：

本計畫未獲通過，本局將維持現行調查、偵蒐與鑑識量能，影響層面評估分析如下：

在數位韌性政府相關政策達成方面，將無法執行「多雲基礎建設、資安戰略規劃、數位系統升級」目標相關策略方法，無法有效應變暫時與急時而實踐「資安即國安」戰略，且無法有效縮減各項資料維護及系統效能維運成本。

在案件調查偵蒐工作方面，調查人員僅能在辦公處所進行批次查詢，並無行動網路及行動應用系統等科技可進行即查即回，若於行動蒐證或搜索現場發現新事證或人證等，將大大降低案件偵辦效率，斲傷政府司法調查量能。

在國家安全工作方面，調查人員僅能透過個別分散或過時不敷實用之系統人工蒐報、判斷、各自查詢或以人脈網絡進行情資瞭解，此極其倚重調查人員經驗，或許會有

時效較長錯失情資掌握與偵辦時機，若能透過系統智慧分析及彙整並進行勾稽關聯，可將原本分段資料進一步綜整為人脈網路分析，獲取有效情資分析，將大大提升國家安全預警能力，降低被滲透之風險。

三、相關機關配合事項：無。

四、中長程個案計畫自評檢核表：如附表三。

五、性別影響評估檢視表：如附表四。

六、其他有關事項：

（一）本計畫如奉核定，將循預算程序提報需求，並視核定預算額度情形依本計畫分期（年）執行策略納入預算編列。

（二）財產採購驗收完畢後，將依規定送本局財產管理單位為財產產籍登記。

（三）附件：本計畫各品項估列金額參考之廠商報價單等相關資料。

附表一-經費需求表

目標	辦理項目		細項		114		114（刪減後）		115		115（刪減後）		116		116（刪減後）		117		117（刪減後）		合計		合計（刪減後）		報價單編號
					總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	
多雲基礎建設	1	建置雙活/多活機房系統	異地機房基礎建設		11,760		11,760														11,760		11,760		114-1
			異地機房軟、硬體設備採購						45,840		45,840										45,840		45,840		115-2
			無人機房 KVM 管理系統		3,465		3,465														3,465		3,465		114-3
			雙活機房網路線路租賃費用						6,000	6,000	6,000	6,000	6,000	6,000	6,000	6,000	6,000	6,000	6,000	6,000	18,000	18,000	18,000	18,000	115-8
	2	建置公有雲分持加密、核心系統與資料備份服務	地端碎形備份節點建置等	地端碎形備份節點建置	600		600														600		600		114-4
				公有雲端備份系統建置					200		200										200		200		
				混合雲加密安全資料備份系統維護及客製化功能增設					2,500		2,500		2,500		2,500		2,500		2,500		7,500		7,500		
				地端備份及公有雲端備份系統介接									150		150						150		150		
				混合雲加密安全資料備份系統									800		800						800		800		
				地端備份及公有雲端備份系統介接													200		200		200		200		
			公有雲備份分持系統						19,294		19,294										19,294		19,294		115-1
			公有雲租賃費用						1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	3,000	3,000	3,000	3,000	115-7
	3	建置加密與金鑰管理系統	加密與金鑰管理系統		10,000		10,000														10,000		10,000		114-2
	4	擴增維運系統監控功能	維運系統監控		2,500	2,500	2,500	2,500	2,500	2,500	2,500	2,500	2,500	2,500	2,500	2,500	2,500	2,50	2,500	2,500	10,000	10,000	10,000	10,000	114-15
	5	建置及防護本局雲端化全球資訊網系統	全球資訊網雲端化 DDoS 防護授權		2,200	2,200	1,320	1,320	2,200	2,200	1,320	1,320	2,200	2,200	1,320	1,320	2,200	2,200	1,320	1,320	8,800	8,800	5,280	5,280	114-30
			全球資訊網雲端化作業系統維運		744	744	720	720	744	744	720	720	744	744	720	720	744	744	720	720	2,976	2,976	2,880	2,880	
			全球資訊網維運技術服務		2,500	2,500	2,250	2,250	2,500	2,500	2,250	2,250	2,500	2,500	2,250	2,250	2,500	2,500	2,250	2,250	10,000	10,000	9,000	9,000	
			雲端化網專業教育訓練		700	700	525	525	700	700	525	525	700	700	525	525	700	700	525	525	2,800	2,800	2,100	2,100	

目標	辦理項目		細項	114		114（刪減後）		115		115（刪減後）		116		116（刪減後）		117		117（刪減後）		合計		合計（刪減後）		報價單編號
				總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	
			本局全球資訊網雲端移轉服務	1,600	1,600	1,200	1,200	1,600	1,600	1,200	1,200	1,600	1,600	1,200	1,200	1,600	1,600	1,200	1,200	6,400	6,400	4,800	4,800	
			本局全球資訊網系統變更開發	885	885	885	885	885	885	885	885	885	885	885	885	885	885	885	885	3,540	3,540	3,540	3,540	
多雲基礎建設 小計(仟元)				36,954	11,129	35,225	9,400	86,963	18,129	84,234	16,400	21,579	18,129	19,850	16,400	20,829	18,129	19,100	16,400	165,325	65,516	158,409	58,600	
資安戰略規劃	1	建置身份管理平台	零信任架構網路設備	33,810		23,810														33,810		23,810		114-5
	2	建置單一簽入管理平台	身份驗證及設備管理系統	6,426		6,426														6,426		6,426		114-6
			身份驗證用指紋碟	399	399	399	399													399	399	399	399	114-16
	3	擴增資安維運	SIEM 整合 SOAR 及視覺化方案	3,000	3,000	3,000	3,000	3,000	3,000	3,000	3,000	3,000	3,000	3,000	3,000	3,000	3,000	3,000	3,000	12,000	12,000	12,000	12,000	114-17
		自動響應功能及建置端點偵測及應變機制	完整端點安全防護系統					15,120		15,120										15,120		15,120		115-
	4	建置與擴增資產管理系統、建置資通安全弱點通報機制及擴增軟體更新系統	資產管理系統、資通安全弱點通報機制及軟體更新系統									4,808	4,808	4,808	4,808					4,808	4,808	4,808	4,808	116-5
	5	擴增資安誘捕防禦系統	資安誘捕防禦系統	10,857		10,857														10,857		10,857		114-7

目標	辦理項目		細項		114		114（刪減後）		115		115（刪減後）		116		116（刪減後）		117		117（刪減後）		合計		合計（刪減後）		報價單編號
					總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	
資安戰略規劃	6	新世代網路電腦犯罪追查軟體授權及鑑識與監控系統設備更新	網路跡證溯源系統設備	NutanixNX-1175S-G7-4210-CM NutanixNX-1175S-G7-4208-CM	656		--		656		--		656		--		656		--		2,624		--		114-8
				NutanixNX-1175S-G8-4208	110		--		110		--		110		--		110		--		440		--		
				Qsan XCubeSAN XS1212S	98		--		98		--		98		--		98		--		392		--		
				Cisco C9300-24T-E	75		--		75		--		75		--		75		--		300		--		
				Cisco ISE 系統(含100 帳號)	35		--		35		--		35		--		35		--		140		--		
			網路跡證溯源系統軟體使用授權	目標脈絡溯源分析系統(目標分析、隱性人員脈絡分析)	1,200	1,200	1,200	1,200	1,200	1,200	1,200	1,200	1,200	1,200	1,200	1,200	1,200	1,200	1,200	1,200	4,800	4,800	4,800	4,800	114-18
				網路跡證追查系統(線索成員分析、跡證追溯、跡證散布分析)	1,200	1,200	1,200	1,200	1,200	1,200	1,200	1,200	1,200	1,200	1,200	1,200	1,200	1,200	1,200	1,200	4,800	4,800	4,800	4,800	
				組織行為蒐證系統(關聯分析、目標關聯網路重疊分析、案關組織分析、多個案關組織重疊分析、follower 關聯分析、多個案關 follower 重疊分析))	945	945	945	945	945	945	945	945	945	945	945	945	945	945	945	945	3,780	3,780	3,780	3,780	

目標	辦理項目		細項		114		114（刪減後）		115		115（刪減後）		116		116（刪減後）		117		117（刪減後）		合計		合計（刪減後）		報價單編號
					總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	
資安戰略規劃	6	新世代網路電腦犯罪追查軟體授權及鑑識與監控系統設備更新	網路跡證溯源系統軟體使用授權	異常活動預警系統(各網路社群節點熱度分析、異常狀況預警)	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90	360	360	360	360	114-18
				戰情室系統(網路跡證相關之決策輔助資訊統計、儀表板呈現、資料視覺化)	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90	360	360	360	360	
				視覺化報表系統(資料下載、資料視覺化)	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45	45	180	180	180	180	
				跡證資料庫(臉書及 twitter 等其他網路資料爬取服務、功能)一年資料訂閱	120	120	120	120	120	120	120	120	120	120	120	120	120	120	120	120	480	480	480	480	
				line 社群頻道監測*訂閱制	780	780	780	780	780	780	780	780	780	780	780	780	780	780	780	780	3,120	3,120	3,120	3,120	
				telegram 頻道監測*訂閱制	400	400	400	400	400	400	400	400	400	400	400	400	400	400	400	400	1,600	1,600	1,600	1,600	
				tiktok 來源擴增*訂閱制	125	125	125	125	125	125	125	125	125	125	125	125	125	125	125	125	500	500	500	500	
				小紅書來源擴增*訂閱制	125	125	125	125	125	125	125	125	125	125	125	125	125	125	125	125	500	500	500	500	
				社群監控機制建置維護費用	59	59	59	59	59	59	59	59	59	59	59	59	59	59	59	59	236	236	236	236	
				暗網 API 搜尋及 1 個雲端帳號	2,520	2,520	2,520	2,520	2,520	2,520	2,520	2,520	2,520	2,520	2,520	2,520	2,520	2,520	2,520	2,520	10,080	10,080	10,080	10,080	
			暗網犯罪情資搜尋系統軟體使用授權		8,500	8,500	8,500	8,500	8,500	8,500	8,500	8,500	8,500	8,500	8,500	8,500	8,500	8,500	8,500	8,500	34,000	34,000	34,000	34,000	114-19
			資安情資管理系統開發與維護		1,500	1,500	1,500	1,500	1,500	1,500	1,500	1,500	1,500	1,500	1,500	1,500	1,500	1,500	1,500	1,500	6,000	6,000	6,000	6,000	114-20

目標	辦理項目		細項		114		114（刪減後）		115		115（刪減後）		116		116（刪減後）		117		117（刪減後）		合計		合計（刪減後）		報價單編號
					總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	
資安戰略規劃	6	新世代網路電腦犯罪追查軟體授權及鑑識與監控系統設備更新	網路鑑識與網路安全監控系統擴充	防火牆 Check Point Quantum1800	1,963	1,963	--	--	1,963	1,963	--	--	1,963	1,963	--	--	1,963	1,963	--	--	7,852	7,852	--	--	114-21
				網路鑑識設備 GPROBOX-M (Dell Poweredeg R750，存儲空間 120T)	3,013	3,013	3,013	3,013	3,013	3,013	3,013	3,013	3,013	3,013	3,013	3,013	3,013	3,013	3,013	3,013	12,052	12,052	12,052	12,052	
				防火牆 Check Point Quantum1535+LTE 模組、網路鑑識設備 GPROBOX-Portable (SuperPortable III，存儲空間 16T)、側錄複製器 DATACOM CTP-1000	2,725	2,725	2,725	2,725	2,725	2,725	2,725	2,725	2,725	2,725	2,725	2,725	2,725	2,725	2,725	2,725	10,900	10,900	10,900	10,900	
資安戰略規劃 小計(仟元)					80,866	28,799	67,929	26,836	44,494	28,400	41,557	26,437	34,182	33,208	31,245	31,245	29,374	28,400	26,437	26,437	188,916	118,807	167,168	110,955	
數位系統升級	1	資安鑑識設備佈建及效能提升	鑑識分析專用筆電		2,090		--		1,805		--		2,090		--		1,520		--		7,505		--		114-9 115-4 116-2 117-1
			實驗室數據資料保存系統	核心交換器	200		200														200		200		114-12 116-4
				L2 資料鏈結層交換器	48		48														48		48		
				巨量資料網路儲存伺服器	450		450						450		450						900		900		
				虛擬化軟體					360	360	360	360									360	360	360	360	115-9
				虛擬化伺服器					1,500		1,500										1,500		1,500		115-6
				破密用伺服器					4,400		4,400										4,400		4,400		
			高階鑑識工作站										6,282		6,282		6,282		6,282		12,564		12,564		116-1
			數位證據資料擷取工具	硬碟複製機													3,881		3,881		3,881		3,881		117-2
				防寫盒													322		322		322		322		

目標	辦理項目		細項	114		114（刪減後）		115		115（刪減後）		116		116（刪減後）		117		117（刪減後）		合計		合計（刪減後）		報價單編號
				總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	
數位系統升級	2	新世代鑑識軟體購置暨授權更新	Cellebrite Premium	5,400	5,400	5,400	5,400	5,400	5,400	5,400	5,400	5,400	5,400	5,400	5,400	5,400	5,400	5,400	5,400	21,600	21,600	21,600	21,600	114-22
			Cellebrite Digital Collector	581	581	581	581	581	581	581	581	581	581	581	581	581	581	581	581	2,324	2,324	2,324	2,324	
			Cellebrite UFED 4PC	14,040	14,040	--	--	14,040	14,040	--	--	14,040	14,040	--	--	14,040	14,040	--	--	56,160	56,160	--	--	
			AXIOM Computer (維護)	2,262	2,262	2,262	2,262	2,706	2,706	2,706	2,706	2,838	2,838	2,838	2,838	2,970	2,970	2,970	2,970	10,776	10,776	10,776	10,776	114-23 115-10 116-6 117-4
			AXIOM Computer (新購)	760	760	760	760													760	760	760	760	
			AXIOM Computer & Mobile	1,274	1,274	1,274	1,274	1,400	1,400	1,400	1,400	1,540	1,540	1,540	1,540	1,694	1,694	1,694	1,694	5,908	5,908	5,908	5,908	
			Graykey Premiere	2,922	2,922	--	--	3,068	3,068	--	--	3,221	3,221	--	--	3,382	3,382	--	--	12,593	12,593	--	--	
			X-ways Forensics (維護)	1,176	1,176	1,176	1,176	1,647	1,647	1,647	1,647	1,809	1,809	1,809	1,809	1,998	1,998	1,998	1,998	6,630	6,630	6,630	6,630	
			X-ways Forensics (新購)	798	798	798	798													798	798	798	798	
			Recon ITR (維護)	62	62	62	62	105	105	105	105	114	114	114	114	126	126	126	126	407	407	407	407	
			Recon ITR (新購)	79	79	79	79													79	79	79	79	
			Recon LAB	63	63	63	63	69	69	69	69	76	76	76	76	84	84	84	84	292	292	292	292	
			Atola Insight Forensics	200	200	200	200	220	220	220	220	242	242	242	242	266	266	266	266	928	928	928	928	
			DVR Examiner (維護)	351	351	351	351	772	772	772	772	850	850	850	850	934	934	934	934	2,907	2,907	2,907	2,907	
			DVR Examiner (新購)	351	351	351	351													351	351	351	351	
			Virtual Forensic Computing	96	96	96	96	105	105	105	105	117	117	117	117	129	129	129	129	447	447	447	447	
			Oxygen Forensic Detective	157	157	157	157	173	173	173	173	190	190	190	190	209	209	209	209	729	729	729	729	
			Passware Kit Forensic	27	27	27	27	29	29	29	29	32	32	32	32	35	35	35	35	123	123	123	123	
			Sensity	3,308	3,308	--	--	3,473	3,473	--	--	3,647	3,647	--	--	3,829	3,829	--	--	14,257	14,257	--	--	
	3	資安鑑識實驗室及六都處檢視操作人員專業訓練	Cellebrite Certified Operator 手機數位鑑識軟體教育訓練	550	550	550	550	550	550	550	550	550	550	550	550	550	550	550	550	2,200	2,200	2,200	2,200	114-27
			Cellebrite Certified Physical Analyst 手機數位鑑識軟體教育訓練	650	650	650	650	650	650	650	650	650	650	650	650	650	650	650	650	2,600	2,600	2,600	2,600	
			EC-Council Computer Hacking Forensic Investigator 資安鑑識調查專家教育課程	325	325	325	325	325	325	325	325	325	325	325	325	325	325	325	325	1,300	1,300	1,300	1,300	114-28
			Certified Ethical Hacker 駭客技術專家教育課程	340	340	340	340	340	340	340	340	340	340	340	340	340	340	340	340	1,360	1,360	1,360	1,360	
	4	數位證據儲存載體增購及配發	行動硬碟 1TB	149	149	149	149	238	238	238	238	324	324	324	324	440	440	440	440	1,151	1,151	1,151	1,151	114-24 115-11 116-7 117-5
			行動硬碟 2TB	210	210	210	210	322	322	322	322	432	432	432	432	550	550	550	550	1,514	1,514	1,514	1,514	
			行動硬碟 4TB	303	303	303	303	459	459	459	459	623	623	623	623	785	785	785	785	2,170	2,170	2,170	2,170	
			硬碟 1TB	58	58	58	58	83	83	83	83	108	108	108	108	130	130	130	130	379	379	379	379	

目標	辦理項目		細項		114		114（刪減後）		115		115（刪減後）		116		116（刪減後）		117		117（刪減後）		合計		合計（刪減後）		報價單編號
					總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	
數位系統升級	4	數位證據儲存載體增購及配發	硬碟 2TB		239	239	239	239	344	344	344	344	460	460	460	460	576	576	576	576	1,619	1,619	1,619	1,619	
			硬碟 4TB		518	518	518	518	680	680	680	680	864	864	864	864	1,064	1,064	1,064	1,064	3,126	3,126	3,126	3,126	
			硬碟 6TB		96	96	96	96	150	150	150	150	208	208	208	208	270	270	270	270	724	724	724	724	
			硬碟 8TB		637	637	637	637	900	900	900	900	1,197	1,197	1,197	1,197	1,495	1,495	1,495	1,495	4,229	4,229	4,229	4,229	
			隨身碟 16GB		11	11	11	11	16	16	16	16	21	21	21	21	26	26	26	26	74	74	74	74	
			隨身碟 32GB		18	18	18	18	24	24	24	24	30	30	30	30	36	36	36	36	108	108	108	108	
			隨身碟 64GB		22	22	22	22	29	29	29	29	36	36	36	36	43	43	43	43	130	130	130	130	
			隨身碟 128GB		29	29	29	29	38	38	38	38	48	48	48	48	58	58	58	58	173	173	173	173	
			隨身碟 256GB		56	56	56	56	75	75	75	75	94	94	94	94	113	113	113	113	338	338	338	338	
	5	維護實驗室資訊整合管理平台系統	實驗室資訊整合管理平台系統擴充—案件管理輔助系統-文字檢索擴充套件		1,001		1,001														1,001		1,001		114-10
			實驗室資訊整合管理平台系統維護		1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,200	1,200	1,200	1,200	1,200	1,200	1,200	1,200	4,400	4,400	4,400	4,400	114-25 115-12 116-8 117-6
			雲端資料取證系統擴充	雲端資料取證系統擴充	315		315														315		315		114-11
				OCR 辨識圖像	525		525														525		525		
				Twitter 資料擷取					525		525										525		525		115-5
				Tik Tok 資料擷取					525		525										525		525		
				IG 典藏擷取									420		420						420		420		116-3
				IG Carousel 擷取									420		420						420		420		
				小紅書資料擷取													525		525		525		525		117-3
			雲端資料取證系統維護		1,037	1,037	1,037	1,037	1,205	1,205	1,205	1,205	1,415	1,415	1,415	1,415	1,583	1,583	1,583	1,583	5,240	5,240	5,240	5,240	114-26 115-13 116-9 117-7
	6	建置API 管理平台	API 管理平台(新建 API 管理軟體工具)		5,560		5,560														5,560		5,560		114-13

目標	辦理項目		細項	114		114（刪減後）		115		115（刪減後）		116		116（刪減後）		117		117（刪減後）		合計		合計（刪減後）		報價單編號
				總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	總經費	經常門	
數位系統升級	7	建置系統效能監控平台	系統效能監控平台(1 年期使用授權)	3,297	3,297	3,297	3,297	3,296	3,296	3,296	3,296	3,296	3,296	3,296	3,296	3,296	3,296	3,296	3,296	13,185	13,185	13,185	13,185	114-29
	8	擴充行動調查暨智慧分析系統	GPU 伺服器 2 套、服務 1 套(包含微服務系統架構、測試環境規劃與建置、局外部系統資料串接與爬蟲機制優化、單一嫌犯犯罪行為 AI 分析、多嫌犯關聯性與集團犯罪行為 AI 分析)	11,625		11,625		11,625		11,625		11,625		11,625		11,625		11,625		46,500		46,500		114-14
數位系統升級 小計(仟元)				65,266	43,452	42,906	23,182	65,252	44,872	42,866	24,291	68,205	46,918	45,207	26,010	73,362	49,207	50,591	27,956	272,085	184,449	181,570	101,439	
合計(仟元)				183,086	83,380	146,060	59,418	195,709	91,401	168,657	67,128	123,966	98,255	96,302	73,655	123,565	95,736	96,128	70,793	626,326	368,772	507,147	270,994	

二-風險評估處理彙總表暨風險圖像表

(一) 風險評估處理彙總表

年度施政目標	重要計畫項目	風險項目	風險情境	現有風險對策	現有風險等級		現有風險值(R)=(L)×(I)	新增風險對策	殘餘風險等級		殘餘風險值(R)=(L)×(I)
					可能性(L)	影響程度(I)			可能性(L)	影響程度(I)	
多雲基礎建設	提升資訊機房可用性	AA01. 發生地震	發生芮氏規模6.9以下之地震	本計畫建立之備援機房，耐震度可達7.0	2	2	4	無	2	1	4
		AA02. 發生火災	發生C型種類火災	本計畫建立之備援機房，消防設備可撲滅A、C、D等類型之火災	1	2	2	無	1	2	2
		AA03. 電纜斷裂	馬路施工不慎挖斷電纜，導致電力中斷	本計畫建立之備援機房，具有不斷電系統與發電機，可於停電時自主發電	1	2	2	無	1	2	2
		AA04. 發電機故障	發電機無法啟動	本計畫建立之備援機房，具有多部發電機，電力供應不受少數發電機故障影響，且每年皆會安排專業機電人員檢修測試	1	1	1	無	1	1	1

年度施政目標	重要計畫項目	風險項目	風險情境	現有風險對策	現有風險等級		現有風險值(R)=(L)×(I)	新增風險對策	殘餘風險等級		殘餘風險值(R)=(L)×(I)
					可能性(L)	影響程度(I)			可能性(L)	影響程度(I)	
		AA05. 空調故障	冷氣無法供應，機房溫度升高	本計畫建立之備援機房，具備雙備援之空調系統，可於主空調系統故障時，由備援空調系統提供冷氣	1	1	1	無	1	1	1
多雲基礎建設	提升資訊服務數位韌性	AB01. 資料毀損	副本資料無法開啟	本計畫所建立之資料儲存採多副本方式，單一副本資料無法開啟，可由其他副本開啟	1	1	1	無	1	1	1
		AB02 資料量不符	副本資料與主本資料檔案大小不符	本計畫所建立之資料儲存採多副本方式，單一副本資料檔案大小有問題，可多重比對其他副本	1	1	1	無	1	1	1
		AB03. 資料竄改	副本資料遭竄改	本計畫所建立之資料儲存採多副本方式，單一副本資料遭竄改，可多重比對其他副本之雜湊值，並還原正確資料	1	1	1	無	1	1	1
	完備驗證及授	AC01. 多因子認證失效	負責多因子認證之伺服器故障	本計畫所建立之多因子認證之伺服器，具雙備援機制，不因故障而中斷服務	1	1	1	無	1	1	1

年度施政目標	重要計畫項目	風險項目	風險情境	現有風險對策	現有風險等級		現有風險值(R)=(L)×(I)	新增風險對策	殘餘風險等級		殘餘風險值(R)=(L)×(I)
					可能性(L)	影響程度(I)			可能性(L)	影響程度(I)	
	權機制	AC02. 多因子認證裝置遺失	個人持有之多因子認證手機遺失	本計畫所建立之多因子認證機制，須經過多道認證手續，不因遺失認證裝置而造成重大危害	1	1	1	無	1	1	1
多雲基礎建設	完善設備與網管機制	AD01. 監控平台故障	負責監控各項設備健康狀態的系統故障	本計畫所建立之監控平台為雙備援機制，若其中一套故障，另一套仍可運作	1	1	1	無	1	1	1
		AD02. 導流設備故障	負責導流網路流量的設備發生故障	本計畫所建立之導流設備為雙備援機制，若其中一套故障，另一套仍可運作	1	1	1	無	1	1	1
		AD03. 網路流量分析設備故障	負責網路流量分析的系統故障	本計畫所建立之網路流量分析為雙備援機制，若其中一套故障，另一套仍可運作	1	1	1	無	1	1	1
	完備應用系統安全	AE01. VPN 系統故障	負責 VPN 安全連線的防火牆設備故障	現有網路防火牆架構均採 HA（High Availability），若其中一套故障，另一套仍可運作。	1	1	1	無	1	1	1

年度施政目標	重要計畫項目	風險項目	風險情境	現有風險對策	現有風險等級		現有風險值(R)=(L)×(I)	新增風險對策	殘餘風險等級		殘餘風險值(R)=(L)×(I)
					可能性(L)	影響程度(I)			可能性(L)	影響程度(I)	
	連線機制	AE02. VPN 系統故障	負責 VPN 安全連線的伺服器故障	現有連線安全伺服器均已虛擬化並有定期備份，故障後可快速還原。	1	1	1	無	1	1	1
		AE03. VPN 連線帳密外洩	VPN 連線的 user 帳密遭竊	本計畫所建立之多因子認證機制，須經過多道認證手續，不因帳密遭竊而造成危害。	1	1	1	無	1	1	1
多雲基礎建設	縮減資安事件預警時間	AF01. 預警系統故障	負責資安事件預警之伺服器發生故障	每日均有專責資安人員負責監控，如有故障可即時處理及復原。	1	1	1	無	1	1	1
		AF02. 預警系統故障	負責資安事件預警之應用程式無法執行	每日均有專責資安人員負責監控，如有預警程式無法執行可即時處理。	1	1	1	無	1	1	1
		AF03. 登入預警系統密碼失效	輸入密碼錯誤次數過多，帳號遭凍結	每日均有專責資安人員負責監控，如有密碼錯誤次數過多，可即時處理。	1	1	1	無	1	1	1
	完成全球資訊網系	AG01. 全球資訊網遭受攻擊	全球資訊網遭受 DDoS 攻擊	本計畫規劃將網域名稱解析伺服器(DNS)及全球資訊網雲端化，以避免 DDOS 攻擊。	3	1	3	無	3	1	3

年度施政目標	重要計畫項目	風險項目	風險情境	現有風險對策	現有風險等級		現有風險值(R)=(L)×(I)	新增風險對策	殘餘風險等級		殘餘風險值(R)=(L)×(I)
					可能性(L)	影響程度(I)			可能性(L)	影響程度(I)	
	統雲端移轉	AG02. 全球資訊網遭受攻擊	全球資訊網首頁遭駭客置換	現已有佈建 CimTrak 檔案完整性監控系統，以防止網頁遭竄改。	1	2	2	無	1	2	2
		AG03. 全球資訊網回應時間過長	同一時間有十萬筆連線本局全球資訊網	本計畫規劃擬採全球資訊網多雲分散式架構，以避免單一點流量過大回應時間過長。	2	1	2	無	2	1	2
資安戰略規劃	提升網路跡證溯源系統利用頻度	AH01. 網路跡證溯源系統故障	網路跡證溯源系統之伺服器發生故障	若內網伺服器故障，廠商提供外網雲端帳號，以因應臨時急迫性交辦任務	1	1	1	無	1	1	1
		AH02. 使用者端筆電遺失	網路跡證溯源系統之使用者端筆電遺失	可透過權限管理系統遠端移除該帳號權限	1	1	1	無	1	1	1
		AH03. 使用者 VPN 連線帳號過期	網路跡證溯源系統之使用者 VPN 連線帳號過期	可透過填寫遠距離工作申請單，單次延長 90 天使用權限，90 天後必需再重新申請	1	1	1	無	1	1	1
		AH04. 使用者 Token 手機遺失	網路跡證溯源系統之使用者 Token 手機遺失	可透過權限管理系統遠端移除該帳號權限。	1	1	1	無	1	1	1

年度施政目標	重要計畫項目	風險項目	風險情境	現有風險對策	現有風險等級		現有風險值(R)=(L)×(I)	新增風險對策	殘餘風險等級		殘餘風險值(R)=(L)×(I)
					可能性(L)	影響程度(I)			可能性(L)	影響程度(I)	
	提升暗網資安情資內容可利用性	AI01. 暗網情蒐系統故障	暗網情蒐系統之伺服器發生故障	每日均有專責人員負責監控，如有故障可即時處理復原	1	1	1	無	1	1	1
		AI02. 暗網情蒐系統無法蒐集資料	來源 IP 被封鎖，導致無法進行搜索	可透過多套 VPN 系統，取得不同 IP，繼續進行情蒐	3	1	3	無	3	1	3
資安戰略規劃	加速大量封包分析能力以強化資安量能	AJ01. 封包分析系統故障	負責封包側錄之設備生故障	與廠商有簽訂保固合約，可進行維修，另有準備緊急備用設備，於設備發生故障，仍可繼續提供服務	1	1	1	無	1	1	1
		AJ02. 封包分析系統故障	負責封包側錄之軟體發生故障，無法運作	設備所需之軟體，皆經原廠授權，若軟體發生故障，可洽原廠工程師修復，或者依照手冊指引重新安裝，避免服務中斷	1	1	1	無	1	1	1
		AJ03. 封包檔案過大	錄製之封包過大，影響分析效能	對封包檔案進行切割，每個子封包檔案以不超過 100MB 為原則	2	1	2	無	2	1	2

年度施政目標	重要計畫項目	風險項目	風險情境	現有風險對策	現有風險等級		現有風險值(R)=(L)×(I)	新增風險對策	殘餘風險等級		殘餘風險值(R)=(L)×(I)
					可能性(L)	影響程度(I)			可能性(L)	影響程度(I)	
	提升資安情資管理系統	AK01. 情蒐數量過低	針對單一事件，24 小時之內蒐集到的件數不如預期	調整關鍵字加上多重搜尋語法，放寬蒐集條件	2	1	2	無	2	1	2
		AK02. 情蒐準確度不足	針對單一事件，卻蒐集到到過多其他關連度較低之事件	調整關鍵字加上複合搜尋語法，限縮蒐集條件	2	1	2	無	2	1	2
數位系統升級	完成 API 管理服務平台建置	AL01. API 管理服務平台發生故障	API 管理服務平台之伺服器發生故障	每日均有專責人員負責監控，如有故障可即時處理復原	1	1	1	無	1	1	1
		AL02. API 管理服務平台發生故障	API 管理服務平台之軟體無法執行	每日均有專責人員負責監控，如有軟體程式無法執行可即時處理	1	1	1	無	1	1	1
		AL03. API 管理服務平台連線中斷	網路設備故障，導致無法與 API 管理服務平台連線	每日均有專責人員負責監控，如有與 API 平台連線之網路設備故障，可即時處理復原	1	1	1	無	1	1	1

年度施政目標	重要計畫項目	風險項目	風險情境	現有風險對策	現有風險等級		現有風險值(R)=(L)×(I)	新增風險對策	殘餘風險等級		殘餘風險值(R)=(L)×(I)
					可能性(L)	影響程度(I)			可能性(L)	影響程度(I)	
	由系統效能監控平台檢出系統問題成因	AM01. 系統效能監控平台發生故障	系統效能監控平台之伺服器發生故障	每日均有專責人員負責監控，如有故障可即時處理復原	1	1	1	無	1	1	1
		AM02. 系統效能監控平台發生故障	系統效能監控平台之軟體無法執行	每日均有專責人員負責監控，如有軟體程式無法執行可即時處理	1	1	1	無	1	1	1
		AM03. 系統效能監控平台連線中斷	網路設備故障，導致無法與系統效能監控平台連線	每日均有專責人員負責監控，如有與系統效能監控平台連線之網路設備故障，可即時處理復原	1	1	1	無	1	1	1
數位系統升級	增進鑑識人員專業能力	AN01. 證據遺失	實體數位證據遺失	相關證據均有專責人員負責保管，工作場域均有監控，門禁進出嚴格把關，故證據遺失之風險極低	1	3	3	以專業設備對數位證據進行完全備份	1	1	1
		AN02. 證據毀損	實體數位證據遭受毀損	相關證據之保存與鑑識，專責人員均受有專業訓練，故證據遭人為毀損之風險極低	1	3	3	以專業設備對數位證據進行完全備份	1	1	1
		AN03. 證據遭竄改	實體數位證據遭受竄改	相關證據之保存與鑑識，專責人員均受有專業訓	1	3	3	以專業設備對數位證據	1	1	1

年度施政目標	重要計畫項目	風險項目	風險情境	現有風險對策	現有風險等級		現有風險值(R)=(L)×(I)	新增風險對策	殘餘風險等級		殘餘風險值(R)=(L)×(I)
					可能性(L)	影響程度(I)			可能性(L)	影響程度(I)	
				練，鑑識時採實體隔離，故證據遭竄改之風險極低				進行完全備份			
	精進數位鑑識及現場取證量能	AP01. 案件過多	單一實驗室需要鑑識之案件件數暴增 20%	透過 AI 分析功能，協助鑑識人員提升鑑識效率，處理案件	1	2	2	無	1	2	2
		AP02. 人手不足	鑑識人員出國參加訓練	透過 AI 分析功能，協助鑑識人員縮短鑑識時間，提升工作處理量能	1	2	2	無	1	2	2

(二) 現有風險圖像表

嚴重 (3)	AN01. AN02. AN03.		
中度 (2)	AA02. AA03. AG02.	AA01. AP01. AP02.	
輕微 (1)	AA04.AA05. AB01.AB02. AB03.AC01. AC02.AD01. AD02.AD03. AE01.AE02. AF01.AF02. AF03.AH01. AH02. AH03. AH04. AI01. AJ01.AJ02. AL01.AL02. AL03. AM01. AM02. AM03.	AG03. AJ03. AK01. AK02.	AG01. AI02.
影響程度 / 可能性	不太可能(1)	可能(2)	非常可能(3)

高度(嚴重)風險： 3項 (7%)

中度風險： 6項 (14%)

低度(輕微)風險：34項 (79%)

(三) 殘餘風險圖像表

嚴重 (3)			
中度 (2)	AA02. AA03. AG02.	AA01. AP01. AP02.	
輕微 (1)	AA04.AA05. AB01.AB02. AB03.AC01. AC02.AD01. AD02.AD03. AE01.AE02. AF01.AF02. AF03.AH01. AH02. AH03. AH04. AI01. AJ01.AJ02. AL01.AL02. AL03. AM01. AM02. AM03. AN01.AN02. AN03.	AG03. AJ03. AK01. AK02.	AG01. AI02.
影響程度 / 可能性	不太可能(1)	可能(2)	非常可能(3)

高度(嚴重)風險： 0項 (0%)

中度風險： 6項 (14%)

低度(輕微)風險：37項 (86%)

附表三-中長程個案計畫自評檢核表

檢視項目	內 容 重 點 (內容是否依下列原則撰擬)	主辦機關		主管機關		備註
		是	否	是	否	
1、計畫書格式	(1)計畫內容應包括項目是否均已填列(「行政院所屬各機關中長程個案計畫編審要點」(以下簡稱編審要點）第 5 點、第 10 點)	V		V		
	(2)延續性計畫是否辦理前期計畫執行成效評估，並提出總結評估報告(編審要點第 5 點、第 13 點)		V		V	
	(3)是否本於提高自償之精神提具相關財務策略規劃檢核表？並依據各類審查作業規定提具相關書件		V		V	
2、民間參與可行性評估	(1)是否評估民間參與之可行性，並撰擬評估說明(編審要點第 4 點）		V		V	本案非屬公共建設且係以「多雲基礎建設」、「資安戰略規劃」及「數位升級」三項目標，導入雲端化、AI 及加密與運算等新興技術而建置與維運相關系統，以期達成數位韌性。因本局業務因涉及犯罪偵查及國家安全，若內容公開後恐造成犯罪者及敵對勢力得窺調查全貌以規避偵查，嚴

檢視項目	內 容 重 點 (內容是否依下列原則撰擬)	主辦機關		主管機關		備註
		是	否	是	否	
						重影響國家安全及犯罪偵辦，且所需經費均來自政府預算支出，故並未開放社會參與及政策溝通
	(2)是否填寫「促參預評估檢核表」評估(依「公共建設促參預評估機制」)		∨		∨	
3、經濟及財務效益評估	(1)是否研提選擇及替代方案之成本效益分析報告(「預算法」第 34 條)		∨		∨	
	(2)是否研提完整財務計畫		∨		∨	
4、財源籌措及資金運用	(1)經費需求合理性(經費估算依據如單價、數量等計算內容)	∨		∨		本案非屬「政府公共建設計畫先期作業實施要點」第 2 點所稱之公共建設計畫。
	(2)資金籌措：本於提高自償之精神，將影響區域進行整合規劃，並將外部效益內部化		∨		∨	
	(3)經費負擔原則： a.中央主辦計畫：中央主管相關法令規定 b.補助型計畫：中央對直轄市及縣(市)政府補助辦法、本於提高自償之精神所擬訂各類審查及補助規定	a		a		
	(4)年度預算之安排及能量估算：所需經費能否於中程歲出概算額度內容納加以檢討，如無法納編者，應檢討調減一定比率之舊有經費支應；如仍有不敷，須檢附以前年度預算執行、檢討不經濟支出及自行檢討調整結果等經費審查之相關文件	∨		∨		
	(5)經資比 1：2 (「政府公共建設計畫先期作業實施要點」第 2 點)		∨		∨	
	(6)屬具自償性者，是否透過基金協助資金調度		∨		∨	
5、人力運用	(1)能否運用現有人力辦理	∨		∨		
	(2)擬請增人力者，是否檢附下列資料： a.現有人力運用情形 b.計畫結束後，請增人力之處理原則 c.請增人力之類別及進用方式 d.請增人力之經費來源		∨		∨	
6、跨機關協商	(1)涉及跨部會或地方權責及財務分攤，是否進行跨機關協商		∨		∨	

檢視項目	內 容 重 點 (內容是否依下列原則撰擬)	主辦機關		主管機關		備註
		是	否	是	否	
	(2)是否檢附相關協商文書資料		V		V	
7、土地取得	(1)能否優先使用公有閒置土地房舍	V		V		本案無涉及土地取得問題。
	(2)屬補助型計畫,補助方式是否符合規定（中央對直轄市及縣(市)政府補助辦法第 10 條）		V		V	
	(3)計畫中是否涉及徵收或區段徵收特定農業區之農牧用地		V		V	
	(4)是否符合土地徵收條例第 3 條之 1 及土地徵收條例施行細則第 2 條之 1 規定		V		V	
	(5)若涉及原住民族保留地開發利用者,是否依原住民族基本法第 21 條規定辦理		V		V	
8、風險管理	是否對計畫內容進行風險管理	V		V		
9、性別影響評估	是否填具性別影響評估檢視表	V		V		
10、環境影響分析(環境政策評估)	是否須辦理環境影響評估		V		V	本案無涉及環境影響分析問題。
11、淨零轉型通案評估	(1)是否以二氧化碳之減量為節能減碳指標，並設定減量目標		V		V	本案無涉及淨零轉型問題。
	(2)是否規劃採用綠建築或其他節能減碳措施		V		V	
	(3)是否強化因應氣候變遷之調適能力,並納入淨零排放及永續發展概念,優先選列臺灣 2050 淨零排放路徑、淨零科技方案及淨零轉型十二項關鍵戰略、臺灣永續發展目標及節能相關指標		V		V	
	(4)是否屬臺灣 2050 淨零排放路徑、淨零科技方案及淨零轉型十二項關鍵戰略相關子計畫		V		V	
	(5)屬臺灣 2050 淨零排放路徑、淨零科技方案及淨零轉型十二項關鍵戰略之相關子計畫者，是否覈實填報附表三、中長程個案計畫淨零轉型通案自評檢核表，並檢附相關說明文件		V		V	
12、涉及空間規劃者	是否檢附計畫範圍具座標之向量圖檔		V		V	本案無涉及空間規劃問題。
13、涉及政府辦公廳舍興建購置者	是否納入積極活化閒置資產及引進民間資源共同開發之理念		V		V	本案無涉及政府辦公廳舍興建購置問題。

檢視項目	內容重點 (內容是否依下列原則撰擬)	主辦機關		主管機關		備註
		是	否	是	否	
14、落實公共工程或房屋建築全生命週期各階段建造標準	是否瞭解計畫目標，審酌其工程定位及功能，對應提出妥適之建造標準，並於公共工程或房屋建築全生命週期各階段，均依所設定之建造標準落實執行		V		V	本案無涉及公共工程問題。
15、公共工程節能減碳及生態檢核	(1)是否依行政院公共工程委員會(下稱工程會)函頒之「公共工程節能減碳檢核注意事項」辦理		V		V	本案無涉及公共工程節能減碳及生態檢核問題。
	(2)是否依工程會函頒之「公共工程生態檢核注意事項」辦理		V		V	
16、無障礙及通用設計影響評估	是否考量無障礙環境，參考建築及活動空間相關規範辦理		V		V	本案無涉及無障礙環境問題。
17、高齡社會影響評估	是否考量高齡者友善措施，參考WHO「高齡友善城市指南」相關規定辦理		V		V	本案無涉及高齡社會影響評估。
18、營(維)運管理計畫	是否具務實及合理性(或能否落實營運或維運)	V		V		
19、房屋建築朝近零碳建築方向規劃	是否已依工程會「公共工程節能減碳檢核注意事項」及內政部建築研究所「綠建築評估手冊」之綠建築標章及建築能效等級辦理		V		V	本案無涉及房屋近零碳建築問題。
20、地層下陷影響評估	屬重大開發建設計畫者，是否依「機關重大開發建設計畫提報經濟部地層下陷防治推動委員會作業須知」辦理		V		V	本案無涉及地層下陷影響評估問題。
21、資通安全防護規劃	資訊系統是否辦理資通安全防護規劃	V		V		

主辦機關核章：承辦人　　單位主管　　首長

主管部會核章：研考主管　　會計主管　　首長

附表四-中長程個案計畫性別影響評估檢視表【一般表】

【第一部分－機關自評】：由機關人員填寫

【填表說明】各機關使用本表之方法與時機如下：

一、計畫研擬階段

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

（二）請運用本表所列之評估項目，將性別觀點融入計畫書草案：

1、將性別目標、績效指標、衡量標準及目標值納入計畫書草案之計畫目標章節。

2、將達成性別目標之主要執行策略納入計畫書草案之適當章節。

二、計畫研擬完成

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

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

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

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

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

計畫名稱：「法務部調查局多雲資安戰略數位升級」中程計畫

主管機關 （請填列中央二級主管機關）	法務部	**主辦機關（單位）** （請填列擬案機關／單位）	法務部調查局

壹、看見性別：檢視本計畫與性別平等相關法規、政策之相關性，並運用性別統計及性別分析，「看見」本計畫之性別議題。

評估項目	評估結果
1-1【請說明本計畫與性別平等相關法規、政策之相關性】	1.本計畫主要係配合政府資安法規、政策關於數位韌性、資安戰略規劃及數

性別平等相關法規與政策包含憲法、法律、性別平等政策綱領及消除對婦女一切形式歧視公約（CEDAW）可參考行政院性別平等會網站（https://gec.ey.gov.tw）。	位系統升級戰略推動，僅針對本局內部維運中各式關鍵基礎設施、軟硬體系統、平台、應用程式及資料之建置、雲端升級、儲存備份、存取權限管理等，整合建置與維運於待建置之雲端安全資訊鏈路及零信任架構環境下，逐年進行自動化、雲端化，因此屬性上著重於資訊軟硬體系統配置與實作，相對較少涉及人力及性別規劃與配置，即於性別平等議題相關性相對上較不顯著，惟依循性別平等政策綱領、性別主流化政策及消除對婦女一切形式歧視公約(CEDAW)之基本精神，自評已盡力妥善規劃並滿足不同性別之各類工作項目決策及規劃執行需求，致力提升環境之性別平等性、友善性與安全性，並且未來加強對執行廠商宣導落實性別工作平等法及就業服務法，營造性別友善空間環境。 2.本計畫藉由採購建置、擴充及維運各式落實數位韌性、資安戰略規劃及數位系統升級目標相關項目，例如雙活機房、分持備份與混合雲戰略、網路跡證溯源、暗網犯罪情資搜尋及行動調查暨智慧分析等系統、雲端中控與API 管理等平台、各式新世代數位鑑識軟硬體設備及本局全球資訊網系統升級雲端化，可期達成「國家安全」及「犯罪防制」兩大使命工作及有效達成

	「確保國家安全」、「維護社會安定」、「保障民眾福祉」之三大願景；因受益者為國家、司法及人民等主體，受偵查或對象均無涉特定性別、性傾向或性別認同者。
評估項目	**評估結果**
1-2【請蒐集與本計畫相關之性別統計及性別分析（含前期或相關計畫之執行結果），並分析性別落差情形及原因】 請依下列說明填寫評估結果： a.歡迎查閱行政院性別平等處建置之「性別平等研究文獻資源網」(https://www.gender.ey.gov.tw/research/)、「重要性別統計資料庫」(https://www.gender.ey.gov.tw/gecdb/)（含性別分析專區）、各部會性別統計專區、我國婦女人權指標及「行政院性別平等會—性別分析」(https://gec.ey.gov.tw)。 b.性別統計及性別分析資料蒐集範圍應包含下列 3 類群體： **①政策規劃者**（例如:機關研擬與決策人員；外部諮詢人員）。 **②服務提供者**（例如:機關執行人員、委外廠商人力）。 **③受益者**（或使用者）。 c.前項之性別統計與性別分析應盡量顧及不同性別、性傾向、性別特質及性別認同者，探究其處境或需求是否存在差異，及造成差異之原因；並宜與年齡、族群、地區、障礙情形等面向進行交叉分析（例如：高齡身障女性、偏遠地區新住民女性），探究在各因素交織影響下，是否加劇其處境之不利，並分析處境不利群體之需求。前述經分析所發現之處境不利群體及其需求與原因，應於後續【1-3 找出本計畫之性別議題】，及【貳、回應性別落差與需求】等項目進行評估說明。	1.政策規劃者： 本計畫奉核准後，將適時召開執行委員會，討論計畫執行議題時，亦將確保所有委員單一性別，不低於三分之一之原則直接參與本計畫之執行，提供寶貴意見，以確保不同性別之權益及性別友善性；另在整體執行過程皆 藉由不同性別之意見，讓計畫全程關注不同性別需求，俾使本計畫完成後能顧及不同性別使用上之便利性與安全性。 2.服務提供者： 本計畫各年度執行策略與分工所需人力，以運用本局各業管單位內及通安全處員額(男女性別比約為1：1)調派共同辦理，包含資安人員、鑑識人員、實驗室人員等；委外廠商人力則主要是機房、各系統軟硬體之建置與專業教育訓練培力講者。 3.受益者(或使用者)： (1)本計畫受益者為國家、司法及人民等主體，並無侷限特定行政區域、場域及案件，受偵查或對象均無涉特定性別、性傾向或

d.未有相關性別統計及性別分析資料時，請將「強化與本計畫相關的性別統計與性別分析」列入本計畫之性別目標（如 2-1 之 f ）。	性別認同者，惟可明確統計出各系統使用者、專業教育訓練培力學員及資安或鑑識證照取得者。
評估項目	**評估結果**
1-3【請根據 1-1 及 1-2 的評估結果，找出本計畫之性別議題】 性別議題舉例如次： **a.參與人員** 政策規劃者或服務提供者之性別比例差距過大時，宜關注職場性別隔離（例如：某些職業的從業人員以特定性別為大宗、高階職位多由單一性別擔任）、職場性別友善性不足（例如：缺乏防治性騷擾措施；未設置哺集乳室；未顧及員工對於家庭照顧之需求，提供彈性工作安排等措施），及性別參與不足等問題。 **b.受益情形** ①受益者人數之性別比例差距過大，或偏離母體之性別比例，宜關注不同性別可能未有平等取得社會資源之機會（例如:獲得政府補助；參加人才培訓活動），或平等參與社會及公共事務之機會（例如:參加公聽會/說明會）。 ②受益者受益程度之性別差距過大時（例如:滿意度、社會保險給付金額），宜關注弱勢性別之需求與處境（例如:家庭照顧責任使女性未能連續就業，影響年金領取額度）。 **c.公共空間** 公共空間之規劃與設計，宜關注不同性別、性傾向、性別特質及性別認同者之空間使用性、安全性及友善性。 ①使用性：兼顧不同生理差異所產生的不同需求。 ②安全性：消除空間死角、相關安全設施。 ③友善性：兼顧性別、性傾向或性別認同者之特殊使用需求。 **d.展覽、演出或傳播內容**	1.本計畫涉及雲端及資安等系統之建置與維運，雖相對未涉及較多空間及工程等議題，惟仍基於使用者角度關注不同性別、性傾向、性別特質及性別認同者之軟硬體設備使用安全性及友善性，未來可視不同人員使用經驗及性別統計資料，持續關注不同性別、性傾向及性別認同者之使用需求並進行改善。 2.本計畫規劃採購各式電腦軟硬體及可攜式行動儲存設備時，將擇選適合使用者身形、承重能力及操作便利性之設備，以期對不同性別、性傾向、性別特質或性別認同者達到便利性、合理性 及安全性的需求。

藝術展覽或演出作品、文化禮俗儀典與觀念、文物史料、訓練教材、政令/活動宣導等內容，宜注意是否避免複製性別刻板印象、有助建立弱勢性別在公共領域之可見性與主體性。 **e.研究類計畫** 研究類計畫之參與者（例如:研究團隊）性別落差過大時，宜關注不同性別參與機會、職場性別友善性不足等問題；若以「人」為研究對象，宜注意研究過程及結論與建議是否納入性別觀點。	
貳、回應性別落差與需求：針對本計畫之性別議題，訂定性別目標、執行策略及編列相關預算。	
評估項目	**評估結果**
2-1【請訂定本計畫之性別目標、績效指標、衡量標準及目標值】 請針對 1-3 的評估結果，擬訂本計畫之性別目標，並為衡量性別目標達成情形，請訂定相應之績效指標、衡量標準及目標值，並納入計畫書草案之計畫目標章節。性別目標宜具有下列效益： **a.參與人員** ①促進弱勢性別參與本計畫規劃、決策及執行，納入不同性別經驗與意見。 ②加強培育弱勢性別人才，強化其領導與管理知能，以利進入決策階層。 ③營造性別友善職場，縮小職場性別隔離。 **b.受益情形** ① 回應不同性別需求，縮小不同性別滿意度落差。 ② 增進弱勢性別獲得社會資源之機會（例如:獲得政府補助；參加人才培訓活動）。 ③ 增進弱勢性別參與社會及公共事務之機會（例如:參加公聽會/說明會，表達意見與需求）。 **c.公共空間** 回應不同性別對公共空間使用性、安全性及友善性之意見與需求，打造性別友善之公共空間。	■有訂定性別目標者，請將性別目標、績效指標、衡量標準及目標值納入計畫書草案之計畫目標章節，並於本欄敘明計畫書草案之頁碼： 1.本計畫擬透過軟硬體設備及應用程式系統之採購與建置，滿足與縮小不同性別、性傾向或性別認同者之使用需求與差異改善之迫切性，並建構便利、友善、安全的使用環境，具體實踐性別平權觀念、改善縮小不同性別、性傾向或性別認同者 差異之迫切性與需求性。 2.性別目標列於本計畫書第 21、24、60 頁，係以「強化與本計畫相關的性別統計與性別分析」及「建構性別友善工作環境與公共空間」為主，且本計畫各年度執行策略與分工所需人力，以運用本局各業管單位內員額調派共同辦理及資通安全處為主

d.展覽、演出或傳播內容 ① 消除傳統文化對不同性別之限制或僵化期待，形塑或推展性 別平等觀念或文化。 ② 提升弱勢性別在公共領域之可見性與主體性（如作品展出或演出；參加運動競賽）。 e.研究類計畫 ① 產出具性別觀點之研究報告。 ② 加強培育及延攬環境、能源及科技領域之女性研究人才，提升女性專業技術研發能力。 f.強化與本計畫相關的性別統計與性別分析。 g.其他有助促進性別平等之效益。	要人力，目前本局資通安全處目前參與及執行本計畫同仁之男女性別比約為1：1，單一性別未低於三分之一，故可視實際需求於適當空間建置相關設施諸如女性夜間人員備勤室或男、女浴廁等，且已考量並關注不同性別參與機會及職場性別友善性，兼顧不同性別、性傾向、性別特質或性別認同者。 3.績效指標、衡量標準及目標值係建立並強化性別統計資料與分析，且以每年主要系統使用、計畫執行者或專業訓練培力講者與學員之性別統計產出率衡量，列於本計畫書第37、40、60及61頁。
評估項目	**評估結果**
2-2【請根據2-1本計畫所訂定之性別目標，訂定執行策略】 請參考下列原則，設計有效的執行策略及其配套措施： a.參與人員 ① 本計畫研擬、決策及執行各階段之參與成員、組織或機制（如相關會議、審查委員會、專案辦公室成員或執行團隊）符合任一性別不少於三分之一原則。 ② 前項參與成員具備性別平等意識/有參加性別平等相關課程。 b.宣導傳播 ① 針對不同背景的目標對象（如不諳本國語言者；不同年齡、族群或居住地民眾）採取不同傳播方法傳布訊息（例如：透過社區公布欄、鄰里活動、網路、報紙、宣傳單、APP、廣播、電視等	■有訂定執行策略者，請將主要的執行策略納入計畫書草案之適當章節，並於本欄敘明計畫書草案之頁碼： 1.本計畫於規劃、設計、建置及使用等階段皆廣納不同性別與族群之使用者意見，以滿足多元化需求，尤其於各階段討論規劃與執行時，皆以「任一性別不少於三分之一」作為性別組成比例考量，並積極培育及延攬女性科技研究人才，且設計性別統計項目表格逐年計進行統計與分析，詳細內容列於本計畫書第60至61頁。 2.本計畫未來進行各項採購時，將於招標文件載明

多元管道公開訊息，或結合婦女團體、老人福利或身障等民間團體傳布訊息)。 ② 宣導傳播內容避免具性別刻板印象或性別歧視意味之語言、符號或案例。 ③ 與民眾溝通之內容如涉及高深專業知識，將以民眾較易理解之方式，進行口頭說明或提供書面資料。 **c.促進弱勢性別參與公共事務** ① 計畫內容若對人民之權益有重大影響，宜與民眾進行充分之政策溝通，並落實性別參與。 ② 規劃與民眾溝通之活動時，考量不同背景者之參與需求，採多元時段辦理多場次，並視需要提供交通接駁、臨時托育等友善服務。 ③ 辦理出席民眾之性別統計；如有性別落差過大情形，將提出加強蒐集弱勢性別意見之措施。 ④ 培力弱勢性別，形成組織、取得發言權或領導地位。 **d.培育專業人才** ① 規劃人才培訓活動時，納入鼓勵或促進弱勢性別參加之措施 （例如:提供交通接駁、臨時托育等友善服務；優先保障名額；培訓活動之宣傳設計，強化歡迎或友善弱勢性別參與之訊息；結合相關機關、民間團體或組織，宣傳培訓活動)。 ② 辦理參訓者人數及回饋意見之性別統計與性別分析，作為未來精進培訓活動之參考。 ③ 培訓內涵中融入性別平等教育或宣導，提升相關領域從業人員之性別敏感度。 ④ 辦理培訓活動之師資性別統計，作為未來師資邀請或師資培訓之參考。 **e.具性別平等精神之展覽、演出或傳播內容** ① 規劃展覽、演出或傳播內容時，避免複製性別刻板印象，並注意創作者、表演者之性別平衡。	並提醒履約廠商應落實並遵守勞動基準法、性別平等工作法及就業服務法等相關規定，以營造性別友善之工作環境。

② 製作歷史文物、傳統藝術之導覽、介紹等影音或文字資料時，將納入現代性別平等觀點之詮釋內容。 ③ 規劃以性別平等為主題的展覽、演出或傳播內容（例如:女性的歷史貢獻、對多元性別之瞭解與尊重、移民女性之處境與貢獻、不同族群之性別文化）。 **f.建構性別友善之職場環境** 委託民間辦理業務時，推廣促進性別平等之積極性作法（例如：評選項目訂有友善家庭、企業托兒、彈性工時與工作安排等性別友善措施；鼓勵民間廠商拔擢弱勢性別優秀人才擔任管理職），以營造性別友善職場環境。 **g.具性別觀點之研究類計畫** ①研究團隊成員符合任一性別不少於三分之一原則，並積極培育及延攬女性科技研究人才；積極鼓勵女性擔任環境、能源與科技領域研究類計畫之計畫主持人。 ②以「人」為研究對象之研究，需進行性別分析，研究結論與建議亦需具性別觀點。	
評估項目	**評估結果**
2-3【請根據 2-2 本計畫所訂定之執行策略，編列或調整相關經費配置】 各機關於籌編年度概算時，請將本計畫所編列或調整之性別相關經費納入性別預算編列情形表，以確保性別相關事項有足夠經費及資源落實執行，以達成性別目標或回應性別差異需求。	■有編列或調整經費配置者，請說明預算額度編列或調整情形： 1. 本計畫經常門中各服務類採購，例如 Cellebrite Certified Operator 手機數位鑑識軟體等教育訓練、本局全球資訊網維運技術服務、雲端化網專業教育訓練、雲端移轉服務、系統變更開發等項目，涉及使用者或廠商來局提供訓練服務人員、專業駐點人員及本局受訓人次與性別及系統維護時間之配置，

	為兼顧不同性別、年齡層、使用便利性、安全性、家庭與工作時間平衡等綜合考量，以營造友善性別環境，已編列相關預算。

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

參、評估結果

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

3-1 綜合說明	一、性別平等專家學者之檢視意見： (一)各項合宜性均合宜，且進一步建議： 1.關於「性別統計及性別分析之合宜性」項目，可逐年建立實際發生案件嫌疑犯、犯罪人之性別統計以利未來分析，且在服務端可建立身分驗證、身份管理系統之使用民眾性別統計，若有年齡、區域統計，未來分析更有效益。 2.關於「綜合性檢視意見」項目，本計畫之執行者，鑑識人員、維運人員、資安人員、實驗室人員、分析室人員、檢視操作人員、資料庫人員等，甚至未來擴增人員，若有明確性別統計資料更佳；於專業訓練培力階段，講授者、學員都要建立性別統計資料，希望不同性別者都有機會被看見、被培力。	
3-2 參採情形	3-2-1 說明採納意見後之計畫調整（請標註頁數）	一、本計畫各年度核心工作之主要參與決策與規劃(執行)者，係以本局資通安全處為主要人力來源，推估可維持男女性別比1:1(即各 50%)而符合「任一性別不少於三分之一」原則，性別目標、績效指標、衡量標準及目標值詳如本計畫書第 21、24、37、40、60 及 61 頁所示。 二、關於性別平等專家學者於「性別統計及性別分析之合宜性」及「綜合性檢視意見」項目之意見，均予採納，修正內容詳如本計畫書 60 至 61 頁，說明如下： (一)就本計畫目標「多雲基礎建設」所涵蓋「多因子認證使用者」、「以安全機制連線應用系統使用者」及「使用者安全存取資料使用者」各使用者或案關對象之「年齡是否屬中高齡(45 歲以上)」、「教育程

		度」及「使用系統或犯罪之行為區域」進行性別統計與分析。 (二)就本計畫目標「資安戰略規劃」所涵蓋「網路跡證溯源系統使用者」、「暗網犯罪情資搜尋系統使用者」及「資安情資管理系統使用者」各使用者或案關對象之「年齡是否屬中高齡(45 歲以上)」、「教育程度」及「使用區域」進行性別統計與分析。 (三)就本計畫目標「數位系統升級」所涵蓋「取得資安專業證照者」、「取得鑑識專業證照者」、「鑑識實驗室人員」、「鑑識分析相關人員專業訓練講者」、「鑑識分析相關人員專業訓練學員」及「行動調查暨智慧分析系統使用者」各使用者之「年齡是否屬中高齡(45 歲以上)」、「教育程度」及「使用系統或犯罪之行為區域」進行性別統計與分析。
	3-2-2 說明未參採之理由或替代規劃	無。
3-3 通知程序參與之專家學者本計畫之評估結果： 已於 112 年 10 月 19 日將「評估結果」及「修正後之計畫書」通知程序參與者審閱。		

· 填表人姓名：劉季涵 職稱：高級分析師 電話：**02-29112241 分機 2924** 填表日期：112 年 11 月 21 日

· 本案已於計畫研擬初期■徵詢性別諮詢員之意見，或□提報各部會性別平等專案小組（會議日期：____年____月____日）

· 性別諮詢員姓名：陳曼麗 服務單位及職稱：行政院性別平等會委員 身分：符合中長程個案計畫性別影響評估作業說明第三點第一款（如提報各部會性別平等專案小組者，免填）

（請提醒性別諮詢員恪遵保密義務，未經部會同意不得逕自對外公開計畫草案）

【第二部分－程序參與】：由性別平等專家學者填寫

程序參與之性別平等專家學者應符合下列資格之一： □1.現任臺灣國家婦女館網站「性別主流化人才資料庫」公、私部門之專家學者；其中公部門專家應非本機關及所屬機關之人員（人才資料庫網址:http://www.taiwanwomencenter.org.tw/）。 ■2.現任或曾任行政院性別平等會民間委員。 □3.現任或曾任各部會性別平等專案小組民間委員。

（一）基本資料	
1.程序參與期程或時間	112 年 9 月 26 日至 112 年 10 月 11 日
2.參與者姓名、職稱、服務單位及其專長領域	陳曼麗，行政院性別平等會第五、六屆委員，專長：公共行政管理、環境管理、婦女及性別、社區營造、食品消費等。
3.參與方式	□計畫研商會議□性別平等專案小組　■書面意見
（二）主要意見（若參與方式為提報各部會性別平等專案小組，可附上會議發言要旨，免填 4 至 10 欄位，並請通知程序參與者恪遵保密義務）	
4.性別平等相關法規政策相關性評估之合宜性	合宜。
5.性別統計及性別分析之合宜性	合宜。建議： 1.可以逐年建立實際發生案件嫌疑犯、犯罪人之性別統計，以利未來分析。 2.在服務端，可以建立身分驗證、身份管理系統之使用民眾性別統計，若有年齡、區域統計，未來分析更有效益。
6.本計畫性別議題之合宜性	合宜。
7.性別目標之合宜性	合宜。
8.執行策略之合宜性	合宜。
9.經費編列或配置之合宜性	合宜。

10.綜合性檢視意見	1.本計畫之執行者，鑑識人員、維運人員、資安人員、實驗室人員、分析室人員、檢視操作人員、資料庫人員等，甚至未來擴增人員，若有明確性別統計資料，更佳。 2.專業訓練培力階段，建議講授者、學員都要建立性別統計資料，希望不同性別者都有機會被看見、被培力。
（三）參與時機及方式之合宜性	合宜。
本人同意恪遵保密義務，未經部會同意不得逕自對外公開所評估之計畫草案。 （簽章，簽名或打字皆可）___陳曼麗__	

附表五-審提意見回復說明對照表

回復行政院相關機關(單位)113 年 1 月 30 日審提意見對照表

行政院相關機關(單位)審提意見	回復說明
內政部 無意見。	敬會。
財政部 一、本計畫所辦事項涉資安防護一節，考量行政院資安產業發展行動計畫，已明定各中長程計畫配置一定比例資安經費，無意見。	一、 敬會。
二、至辦理事項有關資訊設備採購、軟體授權更新及系統維護擴充等，屬機關為精進業務所需資訊設備汰換升級及維護，查法務部前已提報「法務服務智慧轉型計畫」,辦理事項包括系統開發與軟體購置，考量政府財政資源有限，建請法務部通盤檢視所屬機關之需求性及急迫性，排定系統建置或升級優先順序，循年度獲配預算逐年辦理；倘確有必要申請專案計畫寬列預算，涉整體歲出預算配置權責，尊重行政院主計總處意見。	二、 經查，旨揭「法務服務智慧轉型計畫」未包含本中程計畫所列系統開發與軟體購置項目，且評估本中程計畫所臚列項目之建置與採購具有高度重要性及急迫性，其非僅可將其視為機關為精進所掌業務所需資訊設備常態汰換、升級及維護，而是基於調查局依組織法所賦予之與法務部所屬或其他政府機關有明確屬性區隔之實際維護國安、社安及資安執法查調態樣與權能，以及確為「資安即國安」、「戰時數位韌性」等國家及政府戰略推動與落實層級而有與時俱進建置與升級採購之必要性，建請准予本中程計畫專案申請且優先匡列預算

	額度。
數位發展部 一、 本計畫第21頁規劃導入(建置)API管理平臺，應優先針對資料治理及建立資料標準等進行處理，請補充說明現行資料目錄、格式整備或資料標準建立現況，或可參採資料經緯（Data Fabric）等架構技術並研議規劃導入。	一、現行調查局資料係屬結構化資料，均儲存於關聯式資料庫系統(RDBS)中，且系統中的每個資料庫底下的每個資料表皆有詳細的綱要(scheme)用以定義所有欄位名稱、型態及長度。後續將規劃導入資料管理平臺(DataManagement Platform)以連結原有綱要中的定義及調查局業務內容，俾利資料管理。
二、 計畫多處提及導入AI技術，惟未說明導入何種AI技術，如係導入生成式AI技術，亦須遵守「行政院及所屬機關（構）使用生成式AI參考指引」以避免使用之風險，故建議於計畫敘明預計導入之 AI類型及相關配套措施。另請注意AI資料外洩風險，如：系統回應使用者時意外流出，或機器學習程式建立之資料庫，易發生資料在未經授權下被存取，致違反隱私規範及資料外洩。	二、本中程計畫之AI技術將採大語言模型(LLM)訓練語言模型，而後採生成式AI技術，參考訓練結果用以產出內容。又本中程計畫使用生成式AI技術，除遵守旨揭意見「行政院及所屬機關（構）使用生成式AI參考指引」外，亦會遵照「法務部調查局使用生成式 AI 參考指引」，確保資料查詢安全。另對於資料外洩風險，亦將遵照調查局「個人資料侵害事件應變演練計畫表」，嚴格執行作業流程，降低資安風險。

三、「多雲基礎建設」要建置異地機房，請調查局評估為何不能租用雲端機房。	三、鑒於調查局核心系統多為涉及國家安全或案件偵辦之機密或機敏性資料，經內部多次評估決議認為相關系統資料實不適合放置於雲端機房，仍以建置異地機房為宜。
四、建置身分管理與單一登入管理平臺的目的為何？零信任架構並未要求重建這類管理平臺，請釐清。	四、調查局應用系統已有單一登入管理平臺，惟身分驗證授權機制由不同的單位開發後進行個別管理，需建立基於身分生命週期管理機制，包含驗證、授權及帳號管理，是以，藉本本中程計畫進行整合而提供一個基於身分之單一登入平臺進行第一道防護監控，後續以授權管理各系統連線，將可強化身分認證及系統安全性，此除可符合調查局現行系統架構外，亦能符合數位發展部之零信任架構要求。
五、配合行政院推動數位韌性政策，建議將以下工作納入計畫執行：	
(一)以多雲基礎建設重構關鍵設施及全球資訊網系統，建請參考國家資通安全研究院網站共通規範專區所公布「政府機關雲端服務應用資安參考指	五、(一)依審查意見辦理，且基於資安防護與持續提供服務之目的，調查局全球資訊網已於本中程計畫具體規劃將 DNS 雲端

引」,以降低可能之風險;另有關建置 DDoS 攻擊防護，建議調查局亦可適時採用公有雲服務降低 DDoS 攻擊之影響性，包括採用內容傳遞網路(CDN)服務、域名解析伺服器(DNS)代管服務與虛擬等待室(waiting room)等。	化並且採用 CDN 服務,以期能將 DDoS 攻擊之影響降至最低。
(二)有關升級數位跡證鑑識,調查局106年至109年間已陸續建置六都數位證據檢視分析室，另於112年已將資安鑑識實驗室測試場域延伸成立高雄資安鑑識實驗室,為加速中南部地區取得鑑定報告時效,建議優先運用本部已建置之 T-Road 制度,建立本計畫跨域資料傳輸機制,並可依據 T-Road 機制之規格,將各項資料傳輸工作調整以 API 模式進行。	五、(二) T-Road 可提供政府部門跨機關之間的高速資料傳輸，確保資料傳送過程，不受外部侵害或洩漏，調查局會視業務需求與評估資料之機敏性與重要性並基於偵查不公開原則，與資料需求單位進行研議；於符合法規範圍內，針對確實有必要以 T-Road 管道傳輸之資料，必當依照政府資料傳輸平台管理規範辦理。
(三)有關本計畫規劃以 AI 等新興資訊科技促進鑑識分析及系統效能數位升級,強化應用系統數位韌性等工作項,經查似與110年提報之「法務部調查局鑑識科學大樓遷置暨科學偵查檢驗設備精進」中程計畫(112至115年)之偵查設備暨接待陳展空間所需經費說明	五、(三) 本中程計畫以 AI 等新興資訊科技促進鑑識分析及系統效能數位升級，強化應用系統數位韌性等工作項，主要為鑑識相關業務使用，使用場域以實驗室為主要範圍；旨揭110年提報之「法務部調查局鑑識科學大樓遷置暨科學偵查檢驗設備精進」中程計畫(112至115

部分工作項，如：AI 智能語音平臺、智能影像 AI 強化平臺及影像辨識 AI 演算法平臺等作業重複，請釐清。	年)，其 AI 智能語音平臺為用於支援偵蒐活動，協助外勤辦案蒐證，強化反竊聽(錄)之安檢設備效能；智能影像 AI 強化平臺及影像辨識 AI 演算法平臺，為支援處理遠端即時影像及遠程遙控蒐證錄影；是以，兩計畫之 AI 平臺作業僅名稱近似但應用、功能、實施場域迥異，且使用之模組及建構之演算法均不相同，並非重複且無法共用。
六、 請再行檢視績效指標之適當性及明確性，例如：	
(一)本計畫規劃建置雙活機房，而績效指標衡量標準為因應停機之恢復所需工時逐年由20小時遞減至4小時。惟雙活機房之建置效益應可達到零停機，建議設置較具挑戰性之績效指標以明計畫效益。	六、(一)雙活資料中心理論上應能達到零停機之狀態，但是否能做到資料同步及停機後系統即時正常切換運作等，仍尚待建置完成後驗測，尚未驗測完成前仍以保守之4小時為恢復標準，調查局會逐年檢視，將零停機作為最終目標。
(二)「每年機關人員多因子認證強化認證及授權機制增加量」係指機制數或是人員數；「每年使用者以安全機制連線應用系統增加量」係指系統數抑或連線數；另「資安人員之系統使用率」、「案件偵查分析	六、(二)「每年機關人員多因子認證強化認證及授權機制增加量」係指人員數量，「每年使用者以安全機制連線應用系統增加量」係指系統數量，以上說明。「資安人員之系統使用率」、「案件偵查分析量」、「新 API 服

量」、「新 API 服務提供率」、「效能問題報告產出率」等項目，較無法明確衡量執行成效，建議適當調整以利追蹤計畫目標達成情形。	務提供率」及「效能問題報告產出率」等4項指標係以數值呈現，以期透過量化指標，作為年度績效之目標值，若僅檢視單一年度之指標較難反映出績效，若透過逐年比較則具有衡量執行成效之價值。
七、 相關資安採購請多採用國產資安解決方案，以促進我國資安產業加速發展。	七、本中程計畫相關資安採購均恪遵政府法規規定，優先採用國產資安解決方案，以促進資安產業發展。
數位發展部資通安全署	
一、 查本案計畫經費預估新台幣6億2,632萬6千元，請補充說明資安經費投入情形，並請依「行政院資安產業發展行動計畫（107年-114年）」規定，投入至少6%之資安經費。	一、本中程計畫恪遵行政院資安產業發展行動計畫（107年-114年）」規定，投入至少6%之資安經費，經詳細計算，均已符合規定。資安經費投入請詳計畫書之附表：經費需求表所載資安戰略規劃之經費需求。
二、 本計畫涉及開發雲空間應用服務及導入零信任網路架構，建議可參考國家資通安全研究院網站共通規範專區所公布「政府機關雲端服務應用資安參考指引」、「身分鑑別與存取控制參考指引」，以及應禁止使用大陸地區	二、遵示辦理。

(含香港及澳門地區)廠商之雲端服務運算提供者，以降低用雲端服務可能帶來之風險，達成安全採用雲端服務目標。	
三、本計畫涉及資通訊軟硬體與勞務服務採購，為免產生資安疑慮，針對大陸地區廠商及陸籍人士參與、大陸廠牌資通訊產品（含軟硬體及服務)提供及使用等，請確實於未來招標文件中明確規範及檢視。	三、遵示辦理。
四、本計畫第3頁引用「資通安全管理法施行細則」第7條第3款之規定，經查調查局未有維運關鍵基礎設施所必要之業務，爰請該局釐正。	四、業於本中程計畫書第3頁更正為「資通安全管理法施行細則」第7條第1款之規定「一、公務機關依其組織法規，足認該業務為機關核心權責所在。」。
五、查調查局填報資安作業管考系統「111年資通系統與服務資產清冊」中，未見資安誘捕防禦系統(原系統擴增，詳第61頁)，請再確認並落實盤點。	五、資安誘捕防禦系統係111年底建置，故尚未列於「111年資通系統與服務資產清冊」內，將於「112年資通系統與服務資產清冊」填報。
六、調查局提報本署113年度政府科技發展計畫書之「資安威脅獵蒐執法行動計畫」與本計畫皆涉及科技偵查，請說明其差異處。	六、「資安威脅獵蒐執法行動計畫」目的係發展主動式網路防禦，建置新版網安情資研析平臺，以提升外勤處站同仁提報網安情資時效，並與合作夥伴

	建立橫向資安聯繫體系，持續擴充資安聯防領域；本中程計畫科技偵查面，目的係針對調查局資通安全案件調查所需資安設備及相關外部情資，包含中繼站查處所需封包側錄及分析設備、調查資安事件外洩資料情資平臺及假訊息查處追查來源情資系統。
七、 本計畫全球資訊網費用似過高，建議評估合理性。	七、本中程計畫全球資訊網主要執行項目，包含：DDoS防護授權(包含CDN服務)、雲端移轉服務、作業系統維運(包含每年之漏洞修補)、系統變更開發、專業教育訓練，依據行政院國家資通安全會報技術服務中心「政府機關雲端服務應用資安參考指引 (V1.2)」111年8月版，略以：「政府機關…應檢視與控制所採用雲端服務可能之風險，完善雲端服務資安防護計畫。在引導雲端服務時，應成立專案指派人員進行規劃與管理，將雲端服務管理議題納入既有ISMS體系及日常資安管理作業中。在規劃階段，機關應適當分析與評估框架，用以決策最適合之雲端服務部署模型、

	雲端服務種類、雲端服務提供者及雲端服務管理目標與政策，並於此階段明確設定與教育所有相關人員資安角色與責任」可知，例如全球資訊網雲端化維運、系統維護及教育訓練等工作內容不可或缺而需編列相關經費支應，其費用均為必要之支出，且調查局於規劃階段已自行評估及參考各政府機關於雲端類及資安類標案，金額應屬合理；於雲端類標案金額，例如「112年度數位新冠病毒健康證明系統維運暨雲端服務及功能增修案 23,000,000元」、「新北市政府消防局雲端119行動派遣系統(第2期)建置案 10,560,000元」、「災害應變雲端協作平臺系統建置案 39,990,000元」，及資安類標案金額例如「112年資通安全委外服務案 15,750,000元」、「112年資安駭侵溯源分析平台授權訂閱採購案15,000,000元」、「112年至113年資訊安全暨個人資料隱私管理制度維護與驗證及資安健診服務案 8,500,000元」，可見本計畫全球資訊網相較於前揭需求屬

	性近同者之費用，並未過高且具合理性。
國家科學及技術委員會 一、 本計畫之目的係擬導入法務部調查局各項治理、服務及儲存雲端化、異地分持備份、AI、加密運算等相關新興資訊技術，以具體執行「多雲基礎建設、資安戰略規劃、數位系統升級」目標，有效達成「戰時應變」、實踐「資安即國安」戰略及因應AI、AIoT、5G及量子電腦時代所衍生之各項挑戰。本計畫之推動有其必要性。	一、敬會。
二、 本計畫三大目標對接所擬採購之設備宜評估合理性及制定品質控管機制；擬開發之技術不宜從頭研發，宜基於三大目標系統性綜整所有研發項目，以確保各推動事項之成果串接與整合，再檢視其合理性，以確保最終效益可以達成。	二、本中程計畫採購之設備均有其必要性與急迫性，定遵循法規辦理相關事宜，並務求品質優良。所需之核心技術，均遴選業界具多年相關開發經驗之優良廠商參與評選，以確保各推動事項能完成目標，並確保最終效益可以達成。
三、 本計畫所列年度績效目標值過於保守，無法符合國家各階段戰時所需，且宜提供相對應之預期關鍵成果，以利後續成效評核。	三、業依審查意見重新評估並於本中程計畫書第38頁調整績效指標項次第3、4、6項，後續將依照經費規劃安排時程，循序漸進，逐年執行計畫目標，以期達

	成績效。
行政院公共工程委員會 一、 法務部調查局因業務機密性與維護國安及資安重責，為主要資安攻擊目標之一，規劃將原地端機房增加多雲基礎建設，以強化數位韌性，惟亦增加攻擊突破口，建議詳細評估資安風險、規劃系統架構與執行步驟，以確保資通安全。另採購部分，建議參考行政院公共工程委員會(以下簡稱工程會)112年9月25日工程企字第1120022701號『公共工程委員會與數位發展部研訂之「各類資訊(服務）採購之共通性資通安全基本要求參考一覽表」及「資訊服務採購作業指引」』為適當評估考量。	一、 調查局基於業務機密性與維護國安及資安，提出本中程計畫以強化數位韌性，定當仔細評估相關風險、規劃系統架構與執行步驟，依循政府規定之辦法進行採購，以確保整體系統安全。
二、 法務部調查局為資安等級A級機關，規劃多雲基礎建設部分，建議資訊系統轉移至雲端，以及分持備份與混合雲戰略時，請注意資料和隱私保護、雲端供應商評估、分持備份之還原演練以及加密金鑰管理等議題，宜參考雲	二、 調查局為資安等級A級機關，定當嚴格要求資料和隱私保護，並遵守相關資安控制措施，以強化資通安全。

端服務之資訊安全及個資保護主流國際標準之資安控制措施，以強化資通安全。	
三、 依「行政院所屬各機關中長程個案計畫編審要點」第5點第3項第6款規定：「中長程個案計畫涉及資訊系統者，應將資通安全防護納入規劃。」，本計畫「執行策略及方法」臚列眾多工作項目，惟未見相關資安防護內容資料，請補充。	三、 業於本中程計畫書第45頁「執行策略及方法」該節補充修正相關資安防護內容。
四、 該計畫建置及開發後，仍有持續依新增資安風險修補系統之需求，機關辦理採購如涉及後續維護工作者，其後續數年維護服務之價格，建議納入採購標的一併考量分年編列預算支應。工程會107年1月11日工程企字第10700010910號函併請參閱。	四、 修補系統漏洞為持續維持系統安全性之重要關鍵，項目相關執行人員，定當謹遵審查建議事項辦理。
行政院主計總處	
一、整體性意見：有關「多雲基礎建設」目標項下之辦理全球資訊網雲端化維運、教育訓練及防護等經費、「資安戰略規劃」目標項下之擴充網路鑑識與網路安全監控系統，以及「數位系統升級」目標項下之購置	一、 本中程計畫所列採購經費支出係因應調查局任務及本中程計畫多雲、資安戰略、目標達成之需要，配合現階段工作重點覈實編列，如納入例行性設備汰換或經常性費用，在整體預算資源有限下勢將受到排

鑑識所需軟硬體設備、系統及維護、教育訓練等經費，考量屬例行性設備汰換或經常性費用，建議刪除該等經費，不納入計畫辦理。	擠，導致無力支應核心業務所需建置之相關經費；調查局執行國家安全維護工作，在面對愈來愈快速的全球化及資訊化時代，以及對於政府與民間機關不法駭侵攻擊行為密度大幅提高之現況下，有關科技辦案及鑑識蒐證等設備同樣必須與時俱進，方能適時掌握各類犯罪態樣及提升鑑識量能，是以旨揭擴充網路鑑識與網路安全監控系統、購置鑑識所需軟硬體設備、系統及維護、教育訓練等經費之支出有必要性及急迫性，且旨揭全球資訊網雲端化維運、系統維護及教育訓練等採購項於本中程計畫亦具必要性及合理性，其支出係為建立與考驗戰時「數位韌性政府」與落實「資安即國安」戰略並完成多雲基礎建設關鍵設施之關鍵項目及提供驗證予開發所需，綜上說明，爰此建請維持本中程計畫原本之預算額度，以期能順利完成本計畫所預定之相關規劃部署。
二、個別目標意見： （一）有關達成「多雲基礎建設」	二、(一) 1. 調查局為達成「多雲基

目標所需經費1.65億元一節： 1. 本項係調查局為因應戰時攻擊，強化數位韌性，規劃將該局全球資訊網系統，改採雲端架構，並將較不具機敏性之資料及與局內業務關係較低之服務優先雲端化。至其他涉及機敏性資料之重要系統，則擬於外勤處建置異地備援機房。	礎建設」目標，固係擇定外勤可用空間建立及優化異地備援基礎建設，以機敏核心系統之數位韌性為優先考量，再以雲端分持備份為輔，建立資料備份安全，並擇取全球資訊網系統此一局內核心系統為標的優先雲端化，惟調查局之全球資訊網系統所存取及處理資料相較於局內其他核心系統所存取與處理者或許相對較不具機敏性，然並不代表此全球資訊網系統非調查局重要核心系統，其作為提供各方或民眾查詢例如全國外逃通緝犯及民眾主動通報或陳情事項受理等對外雙向服務之特定唯一連結至法務部官網之入口網站、不得因平時或戰時駭侵攻擊等因素導致服務中斷、調查局依組織法重要業務之執行等重要功能，其訊息或資料正常處理與顯示及系統正常維運之系統或應用程式並非不會受到惡意攻擊或駭侵，亦非僅是提供與局內業務關係較低服務之系統，是以，全球資訊網系統相對較不具機敏性、屬於調查局核心系統及前述諸多重要本質，正是其被擇

	取作為本計畫多雲基礎建設之雲端安全鏈路及空間建置時程中賴此隨時驗證及據以修正調整之所需重要系統，其並非如旨揭審提意見述及或歸類為與局內業務關係較低之服務及不具得以優先雲端化性質者，且其現行系統架構並非雲端架構，不利於防護日益密集之DDoS等類型之攻擊，是以有必要於本中程計畫進行包含作業系統之開發、建置與維運，並適時導入本中程計畫所建置之雲端安全鏈路及空間架構發揮驗證角色功能，合先敘明。
2. 經查調查局係因業務涉及外交、國防或國土安全事項列為資通安全等級A級機關，首要應就具機敏性之核心資料強化其數位韌性，惟該局規劃優先將較不具機敏性或非核心業務雲端化，似不合理，仍請該局宜優先強化機敏核心系統之數位韌性，並就各項業務雲端化之必要性、成本效益及類此機關作法妥為評估。又調查局局本部已設有小型備份機房，本案仍請優先運用現行設備，本撙節原則辦理。	二、(一)2.請併參上揭二、(一)1.所述，並說明：調查局作為A級機關且核心系統多為涉及國家安全或案件偵辦之機密或機敏性資料，定當優先強化機敏核心系統之數位韌性，惟以全球資訊網系統優先雲端化仍有誠如前述之擇取局內核心系統供滿足驗證需求之效益及例如可避免戰時遭受攻擊導致服務中斷之數位韌性強化等合理性及必要性。另，調查局局本部雖已設有小型備份機房，惟其現行架構與量能僅能勉予供應現行

	業務應用，考量業務成長性與日俱增並兼顧戰時異地備援需求，現行設備建立異地機房有其必要性，調查局於此並已基於國家財政及撙節原則規劃辦理，非另行購置土地而係以外勤可用空間建立及優化異地備援機房等基礎建設。
(二)有關達成「資安戰略規劃」目標所需經費1.89億元一節： 1. 本項係調查局擬導入零信任架構及端點防護等資安措施；購買網路跡證溯源、暗網犯罪情資蒐尋等網路電腦犯罪追查軟體授權，以及擴充網路鑑識與安全監控系統等。	二、(二) 1.敬會。
2. 查調查局科技計畫「臺灣資安卓越深耕-先進網路鑑識計畫」，期程110至113年度，總經費0.59億元，係辦理網路跡證溯源系統之開發及擴充網路情資等。本計畫辦理將AI技術導入該系統，強化分析功能部分，建議由科技計畫經費支應，或納入公共建設計畫之「數位基礎建設」類別經費辦	二、(二) 2.旨揭科技計畫「臺灣資安卓越深耕-先進網路鑑識計畫」(110至113年度)固係辦理網路跡證溯源系統之開發及擴充網路情資等，對於我國網路輿情、不法情資、網路犯罪相關跡證通聯或傳遞之數位足跡之取得與蒐集，在執法業務如國安案件、選舉案件、假訊息案件等均有其重要性，惟因應愈見

理。	嚴峻及隱密之網路犯罪手法已不足因應，因此本中程計畫之「資安戰略規劃」目標除致力於數位升級與韌性提升成果外，於網路跡證溯源系統開發方面亦積極規劃導入例如AI等先進資訊技術以期有效增進執法人員使用該系統之偵查成果，解決前揭新網路犯罪手法不足因應之困境;惟查,相關技術經費支出如無法及時於114年建置及投入運用，恐無法避免上揭打擊不法業務因經費拮据肇生中斷或難以應處等情，且囿於法規面限制，本中程計畫實不符科技計畫及公共建設計畫之「數位基礎建設」類別相關規範:依據「政府公共建設計畫先期作業實施要點」112.07.18版「二、本要點所稱公共建設計畫應符合下列條件：…(二)計畫總經費中屬經常門者不得超過資本門之二分之一。」及「114年度科技發展計畫申請內容、審查程序及注意事項說明」111.7版「壹、科技發展計畫申請內容說明：二、國科會近年嚴格控管各部會署之提報經費總額，以行政院前

	一年度核定數「零成長」研提」，查本中程計畫總經費中，經常門超過資本門之二分之一，且提報經費總額遠超過法務部114年可提報總額新臺幣1億8千餘萬元，是以，尚難由科技計畫或納入公共建設計畫之「數位基礎建設」類別經費支應辦理，仍以申請社會發展計畫經費供本中程計畫支應為宜。
3. 復查調查局「新世代打擊詐欺策略行動綱領1.5版」辦理購置暗網、黑市暨QQ等通訊軟體不法社群情資分析平臺及大數據資訊分析系統功能強化等，另該局刻正修正通訊保障及監察法，擬於電信事業及公眾電信網路業者設置網路資料保存及分析系統等，所需經費預計達100億元以上，似與本計畫購置網路電腦犯罪追查分析之設備及授權有所重複，建請予以釐清並整併辦理。	(二) 3.「新世代打擊詐欺策略行動綱領1.5版」係針對詐欺不法前、後段偵查環節購置暗網、黑市暨QQ等通訊軟體資源(例如駭客論壇、黑市交易論壇、Telegram、QQ等通訊軟體社群之等不同暗網情資各類來源)，以獲悉不法人士近期動態、竊取及交易之標的，進而獲知預判未來可能衍生風險及危害；本中程計畫之網路電腦犯罪追查分析有別於旨揭打詐行動綱領，目的則係針對不法集團透過詐騙取得我國民眾之「個人基本資料」，並透過暗網社群、黑市等管道作為洗錢、交易之手段，規避我國司法機關查緝，期能機先發掘某部門單位個

	資、內部資訊外洩，並於黑市上出現販售資訊時，即能由執法單位即時追溯調查，同時對有關單位、人員發布預警訊息，是以，兩者屬同性質但不同功能面向屬性之軟體，且為能有效防詐於先期、提升不法各環節不法集團實施之難度及遭查緝之風險、鑒於市售情資分析平臺功能模組尚無法以單一系統有效涵蓋所有不法情資等資料以及所需軟體授權將於113年底到期，若不重新採購將無以為用等諸多考量，期能依本中程計畫購置所需軟體，以擴大查緝面向及切入點，進而降低詐欺犯罪動機。另，關於旨揭修正中通訊保障及監察法及擬於電信網路業者設置網路資料保存及分析系統與經費預估審提意見，由於相關法制面、未來計畫是否順利研提、系統架構內容、採購項及預算等均未完備、確定，尚難據以認定本計畫購置網路電腦犯罪追查分析之設備及授權與之重複，且若調查局已提出之本中程計畫需等待該未來計畫之預算與執行勢必緩不濟急，併評估於電信業者

	端設置系統與所配置軟體與調查局已提出之本中程計畫偵蒐所需不法情資及調取程序與時效性均有明顯差別，故為能有效涵蓋不法情資等社群情資資料源以先期遏阻及打擊各態樣不法行為及境外犯罪，本中程計畫購置網路電腦犯罪追查分析設備及授權實有必要。
行政院外交國防法務處 本案法務部為強化該部調查局之資安防護及數位韌性，爰提報旨揭計畫爭取經費，以進行多雲基礎建設、資安戰略規劃及數位系統升級等相關作業，案內工作項目、計畫期程及經費需求是否覈實，仍請審酌相關機關（單位）意見辦理。	本中程計畫案內工作項目、計畫期程及經費需求，事前均有詳細討論規劃，相關經費皆有經過多方覈實，後續執行定當力求樽節經費並且審酌相關機關意見，全力完成目標。
行政院性別平等處 一、2-1部分：本計畫所定性別目標係以「強化與本計畫相關的性別統計與性別分析」為主，並按「每年主要系統使用、計畫執行者或專業訓練培力講者與學員之性別統計產出率(%)」作為相關預期績效指標等之衡量標準，及製作相關表格俾遂行統計，殊值肯定。另查本計畫機關執行或使用人	一、 遵示辦理，已將「建構性別友善工作環境與公共空間」列為性別目標，並揭示可視實際需求評估於適當空間建置女性夜間人員備勤室或男、女浴廁等，修正如本中程計畫書第24、60頁及87頁表2-1評估結果2。

員涵括鑑識、維運、資安、實驗室、分析室、檢視操作等人員及參加專業訓練之講授者與學員，為回應不同性別對公共場域使用性、安全性及友善性之需求，建議併將「建構性別友善工作環境與公共空間」列為性別目標，視實際需求評估於適當空間建置相關設施諸如女性夜間人員備勤室或男、女浴廁等。 二、性別影響評估檢視表2-2部分：本計畫涉及工程、財物或勞務採購，建議於委託廠商辦理相關業務時，宜酌訂促進性別平等之積極性作法（如將提供員工企業托兒或彈性工時等相關措施列為廠商評選項目，視內容適予給分等），並提醒廠商落實勞動基準法、性別平等工作法及就業服務法等相關規定，以營造性別友善之工作環境。前揭建議請併納入表2-2之評估結果。	二、 遵示辦理，修正如本中程計畫書第 88 頁表 2-2 評估結果 2。
個人資料保護委員會籌備處 一、 查個人資料保護委員會籌備處暫行組織規程第2條第3款及辦事細則第5條第2款所定有關個人資料保護法規訂	一、 本中程計畫或調查局所涉及之個人資料相關蒐集使用，定當恪遵相關法令以及最新規定，以維護並保障個資安全。

修、解釋及協調推動之業務，經行政院112年12月5日院授人組字第11220021931號令，定自113年1月1日施行。囿於上開條款尚未施行，國家發展委員會仍為個人資料保護法之法律解釋主管機關，故針對旨揭計畫涉及個人資料保護法規之解釋適用，尊重國家發展委員會法制協調處所提意見。 二、 至旨揭計畫其餘部分，無意見。	二、 敬會。
國家發展委員會 一、 本計畫多雲基礎建設等三項目標工作事項，其中導入AI技術及新購鑑識實驗室設(施)備等，查法務部執行中之「法務部調查局鑑識科學大樓遷置暨科學偵查檢驗設備精進中程計畫」(112至115年)，採購項目包括AI技術語音、影像強化及辨識平臺及實驗室資訊管理等系統，諸多項目與本計畫似有重疊，請法務部先行釐清本計畫目標、工作項目與上開計畫案差異及關聯性，以避免資源重複配置。	一、旨揭「法務部調查局鑑識科學大樓遷置暨科學偵查檢驗設備精進」中程計畫(112至115年)之鑑識實驗室所鑑定資料屬性及科學技術方法以化學、文書、聲紋、測謊及生物鑑定為主，其AI智能語音平臺為用於支援偵蒐活動，協助外勤辦案蒐證，強化反竊聽(錄)之安檢設備效能；智能影像AI強化平臺及影像辨識AI演算法平臺，為支援處理遠端即時影像及遠程遙控蒐證錄影；本中程計畫以AI等新興資訊科技促進鑑識分析及系統效能數位升級，強化應用

	系統數位韌性等工作項，主要為鑑識相關業務使用，使用場域以實驗室為主要範圍，是以旨揭計畫與本中程計畫鑑識實驗室以手機、電腦主機硬碟及各式數位儲存媒體所承載之多媒體訊息資料屬性及所利用資訊技術確有區別，兩計畫之AI平臺作業縱名稱近似但應用、功能、實施場域迥異，且使用之模組及建構之演算法均不相同，並非重複且無法共用，各實驗室亦有其獨特且獨立運作之管理系統，並無大量或巨量資料或管理系統可共用性及資源重複配置等問題。
二、 本計畫所涉軟硬設備擬購項目係由調查局、資通安全處及資安鑑識科個別報價，為避免各單位建置情形差異過大，宜由法務部統籌擬定共同採購標準或策略，如涉品項相同優先以共同供應契約採購。另購置項目如全球資訊網雲端化維運、系統維護及教育訓練等例行性設備汰換或經常性費用，建議予以刪除。	二、本中程計畫相關擬購項目將遵循政府採購法辦理，所列項目係因應調查局資通安全處未來任務及本中程計畫多雲及資安戰略等目標需要，配合現階段工作重點覈實編列，未涉及與其他單位品項相同需優先以共同供應契約採購，且全球資訊網雲端化維運、系統維護及教育訓練等採購項於本中程計畫具必要性及合理性，其支出係為建立與考驗戰時「數位韌性

	政府」與落實「資安即國安」戰略並完成多雲基礎建設關鍵設施之關鍵項目及提供驗證予開發所需，且依據行政院國家資通安全會報技術服務中心「政府機關雲端服務應用資安參考指引 (V1.2)」111年8月版，略以：「政府機關…應檢視與控制所採用雲端服務可能之風險，完善雲端服務資安防護計畫。在引導雲端服務時，應成立專案指派人員進行規劃與管理，將雲端服務管理議題納入既有ISMS體系及日常資安管理作業中。在規劃階段，機關應適當分析與評估框架，用以決策最適合之雲端服務部署模型、雲端服務種類、雲端服務提供者及雲端服務管理目標與政策，並於此階段明確設定與教育所有相關人員資安角色與責任。」可知，例如全球資訊網雲端化維運、系統維護及教育訓練等工作內容不可或缺而需編列相關經費支應，爰此，仍建請維持本中程計畫原本之預算額度，以期能順利完成本計畫所預定之相關規劃部署。

三、 績效指標部分：預期績效指標包括完備統一驗證及授權機制、設備管理機制及應用系統安全連線機制等年度績效目標值均無變化，未具挑戰性，亦無各績效指標衡量標準計算方式及基準，建請通盤檢視修正並具體補充敘明。	三、業依審查意見修正本中程計畫計畫書第38頁績效指標項次第3、4、6項。
四、 計畫書(第64至65頁)「風險評估」章節，請依「行政院所屬各機關中長程個案計畫編審要點」第5點規定修正為「風險管理」，並請依據「行政院及所屬各機關風險管理及危機處理作業手冊」規定，建立「計畫風險評估及處理彙總表」與「計畫風險圖像」。	四、業依審查意見建立「計畫風險評估及處理彙總表」與「計畫風險圖像」並修正至本中程計畫書第69至78頁。

回復行政院相關機關(單位)113 年 3 月 27 日審提意見對照表

行政院相關機關(單位)審提意見	回復說明
財政部 有關前次建議相關資訊設備採購及系統維護擴充等，循年度獲配預算逐年辦理之意見，經法務部檢討仍維持原規劃，並申請專案優先匡列預算額度一節，涉整體歲出預算配置權責，尊重行政院主計總處意見。	敬會。
數位發展部 原則無意見。	敬會。
行政院公共工程委員會 前於113年1月11日書函復旨揭計畫審議意見，經檢視本次計畫書及意見回復對照表，已依意見回復說明，無新增意見。	敬會。
行政院主計總處 一、有關請刪除購置鑑識所需軟硬體設備、系統與各項維運、教育訓練、防護等例行性汰換經費一節，法務部僅說明倘納入例行性項目，其經費將受排擠，爰維持原提報內容， 考量該等設備係屬調查局平時辦案所需經常性經	一、 (一)法務部調查局職掌國家安全、重大犯罪調查及辦理電腦犯罪防制、資安鑑識及資通安全處理等事項，相關案件辦理情形說明如下： 1. 有關偵辦影響國安之網路駭侵及APT駭客組織在臺活動之中繼站案

費，在政府資源有限下，仍請排列優先順序，於法務部主管預算項下調整支應，不納入計畫辦理。	件，110年為45案、111年為53案、112年為59案，113年截至3月經統計已有18案，顯見是類案件數逐年上升，每案平均網路封包側錄期間為2-4週，為因應調查案量增加趨勢，亟需增加側錄系統軟硬體設備，以延長側錄期間而無須頻繁前往取件，有助於整體工作效率與效能提升。 2. 有關資安鑑識案件(案)經統計109年為755案至112年已增加至1,272案，成長68.48%；鑑識證物(件) 109年3,100件至112年3,897件，成長25.71%；證物容量109年780,562GB至112年10,874,110GB，成長13.93倍，亟需採購相關鑑識軟體，培訓資安辦案人力，俾利就近在六都處級單位完成檢視分析報告、節省送至實驗室之人力時間成本、降低數位證物送鑑影響案件偵辦進度之風險。 (二)現今兩岸及國際情勢變化詭譎，高密度假訊息及資安攻擊威脅瞬息萬變，調查局偵辦資安案件逐年大幅增加，現有人力及軟硬體設備實不足支應，為提升辦案量能，亟需增購、提升各項軟硬體設備、培育訓練資安辦案人力、精進各項系統功能，因相關經費需求龐大，實非調查局及法務部

	基本需求額度內可調整容納。 (三)本案計畫經費經覈實檢討，擬減列1億1,917萬9千元，調整後經費改列5億714萬7千元，調整項目詳如本中程計畫書附表一。 (四)有關「多雲基礎建設」目標項下之辦理全球資訊網雲端化維運、教育訓練及防護等經費之審提意見，補充說明其重要性： 1. 重要性： 旨揭經費與規劃包括調查局官網系統及資料庫雲端化，且比照資料庫採雲端分持備份、多雲與混合雲技術；且為了內部網路部分系統及資料庫而建置內部系統雲端平臺之模擬環境，並預計為未具或相對較低機敏性之線上表單簽核系統試作模擬，例如系統雲端化之系統及資料移轉，自動化移轉之可行性試驗及分析，並建置本土雲、境外雲、進行多雲叢集、多雲移轉之效益評估等，致力於建置現有主機系統與雲端服務混合方案，辦理現行官網之雲端化作業、相關系統與資料庫雲端化，範圍包含：全球資訊網站網頁內容管理系統架構重整，可支援輸出靜態網頁，並包含動態版本異動檢查與歷史網頁回溯功能，及屬調查局內部系統但服務範圍包含全局各外勤處站並涉及全球資訊網站

	業務流程之線上表單簽核系統雲端架構之試作模擬。其中，線上表單簽核系統為達成資料一致性，必須建置資料庫，跨多雲供應商時，避免單一供應商失效，故需建立雲端分持機制；前揭系統因具有資料機敏性相對較低、業務量大的特性，適於擇定為雲端架構模擬標的，除可發掘更多建置過程中可能產生的系統衝擊提早因應外，也可避免機敏資料過度擴張產生的機密性風險。另本中程計畫同時規劃採用多組雲端供應商，避免單一供應商失效造成服務中斷，除目前世界主流三大雲端廠商微軟、谷歌、亞馬遜外，本中程計畫亦包含台灣本土雲端服務國家高速網路中心的雲端運算資源，當多組雲端服務廠商同時供應服務時，需於期初規劃分散式系統的資料一致性，避免後續資料錯亂甚至無法正確回溯，需要耗費更多人力檢查與重新輸入的完整性風險。又，關於DDoS防護授權(包含CDN服務)，在此評估業務上具有不可容忍性,於DDoS與CDN服務之建置過程中，需考量現有系統移轉至雲端的軟體開發改寫，同時也保留地端的機房運算資源，避免境外勢力封鎖台灣外部網路時，本土系統無法自行獨立運作的可用性風險。例如，於2018年與2023年皆有遭受重

	大DDoS攻擊並造成服務中斷，惟僅有使用中斷與外國網路連線的緊急處理措施，未能籌措足夠資源進行完整防護計畫，緊急措施期間甚至已造成國外銀行無法即時至調查局取得最新公告，僅能透過傳統電話方式詢問，是以，衡量該類業務風險屬不可容忍之威脅，爰於本中程計畫中規劃經費著手建置相關防護及相對措施,且旨揭諸如DDoS或CDN服務等業務，目前均未編列固定支出之預算，亟須相關經費支持，以建構調查局官網及內部系統之多雲系統數位韌性、DDoS防護及CDN服務等全方位之資安防護網，參考「雲端原生防護4C」的四個層次架構，提高縱深防禦的能力，例如使用雲端叢集、容器防護等技術運用，在各環節中評估可行性之保護，研擬一套安全性高、自動化強、替代性足及恢復力夠的系統，以因應未來突發性資安事件或備戰需要，實有必要性及合理性，爰此建請納入計畫辦理、支持本次刪修後經費預算額度。 (五)關於「資安戰略規劃」目標項下之擴充網路鑑識與網路安全監控系統之審提意見，補充說明其重要性： 1. 重要性： 該系統建置與擴充採購亟具重要

	性、必要性及合理性，原因在於該系統能提供調查局偵辦資安案件現場調查，針對受駭機關或中繼站的機器之網路封包側錄，並將封包資料存放於雲端，惟現行工作係使用Fortinet防火牆搭配該廠牌外部無線設備作為與調查局雲端之連線系統，近期經揭露通報得知Fortinet設備具有CVE漏洞，顯示該系統極易存有弱點，可遠端執行任意程式碼而為高風險弱點，因此擬將現行雲端連線設備進行更換，並已與廠商研擬另套方案，由局端逐步更換原設備，以避免前揭風險，是以相關需求若未獲經費支持以滿足之，資安風險及危害極大，且針對偏遠地區之中繼站與受駭單位之現地調研，亦有使用雲端功能之必要性與重要影響。再者，為因應新型態犯罪、配合國家及上層機關(法務部/行政院)之政策及進行高風險軟硬體使用之駭侵防治等問題，調查局將更新與設置偵辦網路駭侵事件所需使用系統擬具為重要之資安戰略規劃目標，故本中程計畫案經費使用用途除了不同於一般機關平常所使用之辦公設備採購外，所採購項目皆用於犯罪調查中，爰本中程計畫「資安戰略規劃」目標項下提列之擴充網路鑑識與網路安全監控系統相關採購費用乃屬急迫性與必要性屬性

	之支出，建請支持本次刪修後經費預算額度，以期順利完成相關規劃部署。 (六)關於「數位系統升級」目標項下之購置鑑識所需軟硬體設備、系統及維護、教育訓練等經費之審提意見，補充說明其重要性： 1. 重要性： 旨揭採購項目經費從未納入法務部例行性項目，皆是由其他計畫支應，惟其他計畫將面臨結束或更改項目等問題，致所需經費恐難以為繼，亟需本計畫編列經費執行，並請考量調查局鑑識實驗室係國內第一個數位鑑識實驗室，除承接調查局辦案所需，並協助承辦院檢送鑑案件，如不納入本計畫又未獲法務部主管預算項下，將導致鑑識實驗室無法運作之嚴重後果，無論質或量化影響層面甚廣甚鉅、難以估算。另面對愈來愈快速的全球化及資訊化時代，政府與民間機關不法駭侵攻擊行為密度大幅提高，有關科技辦案及鑑識蒐證等設備同樣必須與時俱進，方能適時掌握各類犯罪態樣及提升鑑識效率，且為因應國際認證需求之轉變以順利維持鑑識實驗室正常運作，例如鑑識軟體Encase等鑑識軟體，原本數年前是國內鑑識軟體龍頭，最近卻因不敷前述認證需求已幾乎沒單位在使用，致鑑識

	實驗室於去年必須採購Deepfake偵測軟體Sensity及Reality Defenders以因應之，故隨時代變遷購入最新型鑑識設備有其必要性。更甚者，謹再次重申調查局鑑識實驗室如不納入本計畫又未獲法務部主管預算項下，將導致本實驗室無法運作之嚴重後果，並請依據行政院所屬各機關中長程個案計畫編審要點第三條第一項所揭示計畫類別「社會發展計畫：為預防、解決社會問題，促進社會發展，所研擬具前瞻性、新興性及重大性之計畫」及行政院重要社會發展計畫先期作業實施要點第二條所揭示社會發展計畫特性之核心價值及要求，本中程計畫之鑑識實驗室為因應日益多變的鑑識需求，積極增項實驗室認證(App檢測需要CEH及CHFI證照，詳見本計畫書第51頁)、因應打詐或新型態犯罪亟需拓展六都鑑識量能(增配鑑識、破密軟體及相對應之教育訓練)、鑑識操作流程導入自動化(詳見本計畫書第11頁)等，皆具備未來發展性且為資安鑑識實驗室發展之新興項目，須於本中程計畫匡列經費方能達成，爰此建請納入計畫辦理、支持本次刪修後經費預算額度。

二、有關達成「多雲基礎建設」目標所需經費1.65億元一節，查調查局刻正研擬大型證物庫房、資訊設備異地備援機房及檔案庫房設置計畫，規劃於新北市調查處辦公廳舍原址 設置該局資料中心備援機房，似與本計畫設置異地機房重複，仍請該局補充說明，其備分、備援機房設置之完整規劃。	二、本中程計畫規劃高雄市調查處現有機房優化成為主要備份及備援機房，其提出時程在新北市調查處研擬大型證物庫房及資訊設備異地備援機房之前；新北市調查處原址爭取成為備援機房後，為利維運，未來規劃新北調查處原址為備援機房，高雄市調查處為備份機房，將備份與備援分處不同地方，以增加數位韌性。新北市調查處辦公廳舍原址現階段僅為空間保留規劃，有關備援機房經費將另案辦理。另本中程計畫有部分經費，係用於分散式地端與雲端備份之整合研究，旨在增加另一種備份思維，提供為未來備份選項之一，以增加數位韌性目標。再就備份、備援機房設置之完整規劃補充如下：目前調查局沒有備援機房，僅有高雄處及局本部有機房及儲存空間可供備份，現有200多個系統360多台虛擬機或實體機需要備份，因現有備份資源有限，故備份政策分為三級，金級的是重要系統每日在局本部與高雄定時備份數量約29台，銀級的是次要系統每日於局本部備份約36台，銅級的係較不重要之系統每週於局本部備份一次約34台，其餘的系統每月做一次性完整備份於局本部，如前所

	述大部分系統還是本地備份並無異地備份，因此本中程計畫主要是要改善高雄機房；高雄機房現有環境無交換式空調、UPS不斷電系統、環境偵測系統等均亟需改善，因此本中程計畫係改善高雄機房環境，增加高雄機房可異地備份的容量以分擔局本部備份的負擔，希望以上所有系統均可備份於高雄機房，另本中程計畫也會測試高雄機房成為備援機房是否可行，但因備援成本極高，故於測試階段僅會挑選1個核心系統作測試。至於新北處之規劃原則上以備援機房為優先，調查局現有核心系統約15個，需即時同步的的虛擬機約20～30台，如新北處之土地順利取得，將會規劃為調查局核心系統之備援機房，並將本中程計畫測試的經驗複製於新北機房，若新北機房環境還有餘裕，後續應也可成為第二備份機房，增加調查局的數位韌性，另因新北房舍規劃本局總務處114年僅編列房舍修繕經費，未含機房環境建設及備援設備之費用，故115年將另向法務部爭取機房環境建設經費，如於115年新北機房完工，則本中程計畫採購之備援設備則可搬移至新北機房使用。

三、有關達成「資安戰略規劃」目標所需經費1.89億元一節： （一）有關法務部補充說明，國家科學及技術委員會（以下簡 稱國科會）近年嚴格控制各部會屬之提報經費總額，以行政院前一年度核定數「零成長」研提，爰本案計畫無法調整容納於該部科技預算額度內。考量國科會之規定，係考量政府資源有限，請各部會確實檢討各項計畫實需，並排列優先順序辦理，爰本計畫辦理將AI技術導入網路跡證溯源系統，強化分析功能部分，係屬科技計畫性質，建議仍應請該部檢討於主管科技預算內調整容納。	三、(一)旨揭本中程計畫辦理將AI技術導入網路跡證溯源系統，強化分析功能部分，調查局已刪修部分相關經費，詳如本案附表一所示，並說明其性質與內涵符合行政院所屬各機關中長程個案計畫編審要點第三條第一項所揭示計畫類別「社會發展計畫」及其應具前瞻性、新興性及重大性核心價值及要求，其能否賡續開發及導入先進技術攸關我國網路輿情、不法情資、網路犯罪相關跡證通聯或傳遞之數位足跡之取得與蒐集，在執法業務如國安案件、選舉案件、假訊息案件等均有其重要性，且因應愈見嚴峻及隱密之網路犯罪手法與海量資訊，新興資訊科技技術之導入亦可有效增進執法人員使用該系統之偵查成果，並在114年及時建置及投入實務運用；考量科技計畫、公共建設計畫等經費已超出113年提報時程，無法及時於114年建置及投入運用恐難避免上揭打擊不法業務因經費拮据肇生中斷或難以應處等情與窘境，期仍以本中程計畫支應。
(二)至有關本計畫購置網路電腦犯罪追查分析之設備及授權，與打擊詐欺及通訊	三、(二)旨揭修正中通訊保障及監察法及擬於電信網路業者設置網路資料保存及分析系統與經費預估

保障及監察法相關經費有所重複一節，考量通訊保障及監察法相關經費預計納編114年度預算，又本次調查局未明確敘明三者功能上之差異情形，建請該局再予以補充說明。	審提意見，係屬調查局通訊監察處研提中之計畫內容，惟查，就相關法規範內容而言，依循通訊保障及監察法規定，須為三年以上有期徒刑犯罪與具有具體犯罪事實，並且符合調取作業程序，方能取得電信系統所產生之發送方、接收方之電磁紀錄，而調查局資通安全處職司偵辦電腦犯罪案件、網路駭侵案件、影響國安社安假訊息等工作，關於網路駭侵案件之偵查，常涉及到網路匿蹤及鑑別境外攻擊手法不易之狀況，需仰賴專業情資公司於暗網中蒐集相關資料，例如虛擬通貨交易需要到交易所換取法定貨幣，即可透過蒐集暗網錢包過去的活動以發掘某些不法行為，因此更為注重進入暗網後的資料蒐集，故與調查局通訊監察處處理資料及業務屬性不同，宜請優先支持本項目以提升資安戰略規畫之整體最大利益。 另針對與打擊詐欺相關經費差異，說明如下： 「新世代打擊詐欺策略行動綱領1.5版」係針對詐欺不法前、後段偵查環節購置暗網、黑市暨QQ等通訊軟體資源，以獲悉不法人士近期動態、竊取及交易之標的，期能預判未來可能衍生風險及危

	害，惟相關系統軟體將於113年11月授權到期無法使用;「打擊詐欺策略」則係針對明網及暗網之網路駭侵資訊，情資內容可涵蓋較廣泛網路空間威脅，包含網路犯罪、網路間諜行為等網路攻擊，並具有專門情資分析人員，可得到較完整、邏輯性之情資內容，故可藉由該平臺獲取對網路威脅的深入了解，並採取相應的防禦措施；本中程計畫所購置網路電腦犯罪追查分析有別於前揭兩項，係針對不法集團透過詐騙取得我國民眾之「個人基本資料」，並透過暗網社群、黑市等管道作為洗錢、交易之手段，規避我國司法機關查緝，期能機先發掘某部門單位個資、內部資訊外洩，並於黑市上出現販售資訊時，即能由執法單位先期發覺並即時追溯調查，同時對有關單位、人員發布預警訊息；綜上所述，該些計畫採購項目屬同性質但不同功能面向屬性之軟體，且為能有效防詐於先期、提升不法各環節不法集團實施之難度及遭查緝之風險、鑒於市售情資分析平臺功能模組尚無法以單一系統有效涵蓋所有不法情資等資料，以及所需軟體授權將於113年底到期，若不重新採購將無以為用等諸多考

	量，期能依本中程計畫購置所需軟體，以擴大查緝面向及切入點，進而降低詐欺犯罪動機。
(三)有關達成「數位系統升級」目標所需經費2.72億元一節， 查調查局打擊詐欺相關經費，113年度預算編列1,220萬元 及114年度提報1,888萬8,000元，辦理購置行動調查暨智慧分析系統，與本計畫「數位系統升級」目標項下辦理擴充行動調查暨智慧分析系統似有重複，建議予以釐清。	三、(三)經查114年提報打擊詐欺經費包括有：1.特規行動調查筆記型電腦360萬，2.案件查詢系統升級500萬，3.存取控管軟體授權450萬，4.端點偵測與回應系統578萬8,000元，總計1888萬8,000元，其中項目1屬使用者硬體設備優化，3、4屬使用者安全管控軟體，均與中程計畫系統升級無關；另113年度及114年度提報辦理購置行動調查暨智慧分析系統所包含軟體，其中113年度係建置後台管理平台，用於查調系統使用狀況及產出報表，114年度規劃整合本局單一窗口新架構及新增特權管理者身分切換功能，便於日後維運所需，此兩部分均與本計畫「數位系統升級」目標項下辦理擴充行動調查暨智慧分析系統之 AI 分析無功能重複之處，詳參本中程計畫例如第20、30、45頁可知，即本計畫「數位系統升級」目標項下辦理擴充行動調查暨智慧分析系統之AI 分析功能，係因行動調查系統資料係案件偵辦過程中

	機敏資料，故所有經由 AI 分析產生的行為模式資料，都將經由資料庫加密技術儲存於資料庫中，而所建置 AI 新功能包含「單一嫌犯犯罪行為 AI 分析，透過 AI 相關技術及結合本局內既有資料庫，針對單一嫌犯找出其可能的犯罪行為模式，例如出入境異常、金流異常及出入港異常等等；及應提供多嫌犯關聯性與集團犯罪行為 AI 分析，透過 AI 相關技術及結合調查局內既有資料庫，先找出各嫌犯之間的集團關聯性，例如出入境相關、金流相關及入出港記錄及三親等、工作同事、軍中同袍、股東及獄友等關係，再給予綜合評分且列出所述評分各屬性之權重分數」，此並未重複提報於打擊詐欺經費中。
國家科學及技術委員會 一、本案推動「多雲基礎建設」、「資安戰略規劃」、「數位系統升級」等三大主軸，以提升數位韌性。各主軸之推動方向尚屬可行，並已逐一針對前次審查建議事項正面回應，後續宜如期如實推動。 二、本案在智慧化系統建立面	一、 遵示辦理。 二、本中程計畫智慧化系統建立與開

向，宜與目前推動之相關科技專案密切交流，以達綜效。此外，建議本計畫針對未來應用面提供預期系統運作流程，打造以設計安全(Security by Design)為軸心，強化各整體系統之韌性。	發，於研提初期即評估與相關科技專案之異質性且排除同質性以避免重複，故預期可有互補性與相關綜效；且於軟體生命週期已考量旨揭設計安全原則，即有將程式碼開發、版本控制、資料安全等納入考量，以強化各整體系統之韌性，例如本計畫開發實作之網路溯源跡證系統，於承攬廠商雲端部署爬蟲程式，前臺系統介面及爬取所得資料庫以落地方式建置於本局內部網路，藉此兼顧搜尋資料源具廣度及即時性，以及確保爬蒐相關操作具相當保密性，並保留資料後續運用彈性，至於系統功能模組、細部分析流程，則由調查局人員依實務經驗提出需求後，再由廠商實作開發，後經局內人員投入實務工作加以測試及賡續優化，整個系統亦具體包含：於系統正式上線前須經過OWASP10等系統弱點掃描，確認系統並未包含中高風險等級的弱點後，方能正式上線，並每季針對平臺安排及進行前揭弱點掃描至少一次；系統須記錄平臺使用帳號密碼登入情形，並配合調查局資安政策針對帳號密碼異常登入行為作LINE或EMAIL之告警通知；以及系統連線網址須具備加密機制(例如：SSL)，透過HTTPS方

	式連線至網頁操作系統。
三、本案部分最終預期指標值停在80%(117年度)，倘無法提供所有需求者使用(100%)，是否能達到提高數位韌性之目標，需再斟酌。	三、已依審提意見將本中程計畫書第38頁旨揭指標第3、4、6項修正為100%，以期達成提高數位韌性及零信任等資安戰略規劃目標。
數位發展部資通安全署 一、查本計畫規劃連續4年且每年862.9萬元，辦理現行官網之雲端化作業，惟未說明是否包括相關系統或資料庫雲端化;另，一般官網內容應多為公開資料，是否需要比照資料庫採雲端分持備份、多雲與混合雲技術；又DDoS防護授權(包含CDN服務)等業務較屬年度固定支出，建議先衡量業務可容忍情形，進一步評估經費及相對措施之合理性。	一、 旨揭經費與規畫，包括相關系統或資料庫雲端化，且需要比照資料庫採雲端分持備份、多雲與混合雲技術之原因，謹說明如下：本中程計畫規劃4年各862.9萬元，該經費除用於辦理官網之雲端化作業外，尚包括為了內部網路部分系統及資料庫而建置的內部系統雲端平臺之模擬環境所需，並預計為未具或相對較低機敏性之線上表單簽核系統試作模擬，例如系統雲端化之系統及資料移轉，自動化移轉之可行性試驗及分析，並建置本土雲及境外雲等，更可進行多雲叢集、多雲移轉之效益評估等，故本中程計畫非僅限於為官網之公開資料。換言之，本中程計畫致力於建置現有主機系統與雲端服務混合方案，辦理現行官網之雲端化作業、相關系統與資料庫雲端化，範圍包含：全球資訊網站網頁內容管理系統架構重整，可

	支援輸出靜態網頁，並包含動態版本異動檢查與歷史網頁回溯功能，及屬調查局內部系統但服務範圍包含全局各外勤處站並涉及全球資訊網站業務流程之線上表單簽核系統雲端架構之試作模擬。線上表單簽核系統為達成資料一致性，必須建置資料庫，跨多雲供應商時，避免單一供應商失效，故需建立雲端分持機制。前揭系統因具有資料機敏性相對較低、業務量大的特性，適於擇定為雲端架構模擬標的，除可發掘更多建置過程中可能產生的系統衝擊提早因應外，也可避免機敏資料過度擴張產生的機密性風險。另本中程計畫同時規劃採用多組雲端供應商，避免單一供應商失效造成服務中斷，除目前世界主流三大雲端廠商微軟、谷歌、亞馬遜外，本中程計畫亦包含台灣本土雲端服務國家高速網路中心的雲端運算資源。當多組雲端服務廠商同時供應服務時，需於期初規劃分散式系統的資料一致性，避免後續資料錯亂甚至無法正確回溯，需要耗費更多人力檢查與重新輸入的完整性風險。 又，關於DDoS防護授權(包含CDN服務)，在此評估業務上具有不

	可容忍性，謹說明如下：DDoS與CDN服務之建置過程中，需考量現有系統移轉至雲端的軟體開發改寫，同時也保留地端的機房運算資源，避免境外勢力封鎖台灣外部網路時，本土系統無法自行獨立運作的可用性風險。例如，於2018年與2023年皆有遭受重大DDoS攻擊並造成服務中斷，惟僅有使用中斷與外國網路連線的緊急處理措施，未能籌措足夠資源進行完整防護計畫，緊急措施期間甚至已造成國外銀行無法即時至調查局取得最新公告，僅能透過傳統電話方式詢問，是以，衡量業務可容忍情形後，此應屬不可容忍之威脅，爰於本中程計畫中規劃經費著手建置相關防護及相對措施，具合理性；且旨揭諸如DDoS或CDN服務等業務，目前均未編列固定支出之預算，係以其他業務費用暫時勻支，以現階段環境及技術層面，除屬不可容忍之威脅，亦屬有必要與其他方法共同建置及評估效益之措施，因此所需經費尚屬合理。 綜上所述，併予說明：本中程計畫以建構調查局官網及內部系統之多雲系統之數位韌性為主要精神，DDoS防護及CDN服務等

	僅為資安防護一環，近來資安架構及相關技術日異月新，為本中程計畫建構全方位之防護網，應實際應用及評估各項技術之差異，參考「雲端原生防護4C」的四個層次架構，提高縱深防禦的能力，例如使用雲端叢集、容器防護等技術運用，在各環節中評估可行性之保護，研擬一套安全性高、自動化強、替代性足、及恢復力夠的系統，以因應未來突發性資安事件或備戰需要，實有必要性及合理性，建請仍依原提報經費專案匡列。
二、查本計畫依據之一為國家資通安全發展方案，第七期國家資通安全發展方案刻正規劃中，新興科技犯罪偵防及資安駭侵事件防護亦為延續性重點工作，本計畫相關資安駭侵及新興科技偵查等作為，如：調查資安事件外洩資料情資平臺及假訊息查處追查來源情資系統建置及效益，亦請後續納入第七期國家資通安全發展方案具體措施，以利完備國家整體資通安全範疇。	二、本中程計畫相關資安駭侵及新興科技偵查等作為與採購項目，例如調查資安事件外洩資料情資平臺及假訊息查處追查來源情資系統等，透過資安事件外洩資料情資平臺蒐整暗網資訊，有助各項犯罪調查工作之推動，例如調查局於113年度發現我國重要半導體上市櫃公司、政府交通運輸機構資料等3案外洩情資，並於第一時間交由外勤處站協助偵辦，並透過假訊息查處追查來源情資系統即可針對特定案關跡證，進行時間脈絡橫向及縱向連結，協助局本部第一線承辦同仁，追查案件起源點及影響層面，並撰寫30餘件調查報告，針對聯合

	造假、擴散訊息源頭，供其他司法單位參處應用，達成國家整體資安全縱深防禦，亦同時發布新聞曉諭國人，以強化對不實訊息之監管，維護社會秩序安定。是以，例如上揭兩系統，均具有科技偵辦案件工作推動及經費必要性，倘無法獲得本中程計畫經費支應，相關資安、社安與國安工作將發生停擺之不可承擔嚴重後果，相關工作成效亦勢必歸零，影響甚鉅。 況查，第七期國家資通安全發展方案計畫已於113年3月20日審核通過而評估無法供旨揭項目及經費納入與支應，且旨揭項目性質及經費額度亦符合行政院所屬各機關中長程個案計畫編審要點第三條第一項所揭示計畫類別「社會發展計畫：為預防、解決社會問題，促進社會發展，所研擬具前瞻性、新興性及重大性之計畫」及行政院重要社會發展計畫先期作業實施要點第二條所揭示之社會發展計畫特性：「(一)前瞻性：具有展望未來社會發展之議題。(二)新興性：具有創新且非屬經常性或延續性辦理之議題。(三)重大性：具有對社會發展層面產生重大影響之議題。」之核心價值及要求，綜上而言，雖第七期國家資通安全發展方案亦以新興科技犯罪偵防及資安

	駭侵事件防護為重點工作，惟調查局於本中程計畫相關資安駭侵及新興科技偵查作為與項下經費之研提與獲得支持，係有及時支應、系統開發與延續應用上刻不容緩之屬性，特別是對於攸關我國網路輿情、不法情資、網路犯罪相關跡證通聯或傳遞之數位足跡之取得與蒐集，在執法業務如國安案件、選舉案件、假訊息案件等均有其重要性，亦為現代網路不法證據蒐集、溯源調查之必要系統，且例如因應愈見嚴峻及隱密之網路犯罪手法、海量資訊及生成式AI所衍生犯罪內容偵蒐，非仰賴人工而不導入AI相關技術即可完成，故法務部及調查局評估均認為本中程計畫無法調整容納於部內科技預算額度內，仍以本中程計畫支應為當，爰建請仍以本中程計畫支應，以期適時符合執法單位所需，並避免未及時延續相關偵查作為之重大影響與危害。
行政院外交國防法務處 本案法務部業依國家發展委員會113年1月30日函送相關機關（單位）意見，研提回應說明與修正旨揭計畫內容，其針對達成多雲基礎建設、資安戰略規劃及數位系統升	敬會。

級等強化數位韌性目標，所配合購置軟硬體設備、進行系統擴充升級等項目與經費，是否確具必要性及合理性，仍請參考相關機關（單位）意見審酌。	
行政院性別平等處 無意見。	敬會。
個人資料保護委員會籌備處 旨揭計畫涉及多種系統更新及資料庫擴充事宜，其中若有涉及個人資料之蒐集、處理及利用，亦請注意符合個人資料保護法等相關規定。	遵示辦理。