法務部調查局

多雲資安戰略數位升級中程計畫

成本效益分析報告

中華民國 113 年 10 月

法務部調查局多雲資安戰略數位升級中程計畫

成本效益分析報告

壹、計畫緣起

一、依據

行政院113年6月28日院臺法字第1131013360號函辦理

二、問題研討

1. 自民國(下同)107年美中貿易戰起，再到俄烏戰爭，不斷加劇能源及通膨等問題，國與國之間緊張的地緣政治關係，凸顯國家政策及數位科技扮演的重要角色，因此唯有及早加強「數位韌性」，才能更有效因應全球政經情勢變遷並降低資安攻擊事件所帶來的衝擊影響。
2. 就本局而言，以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，還能持續提供資訊服務，並同時確保本局司法調查資訊中心可賡續運營。
3. 近年來量子運算技術的快速進展，對現今加密與解密技術帶來巨大衝擊，因量子電腦可以快速突破特定演算法的加密技術，可預期在未來將更容易破解密碼，因此密碼防護

開始朝向後量子密碼學（Post-quantum cryptography，PQC）的研究，發展可抵抗量子電腦破解的加密演算法。本計畫希透過與民間專業密碼研究團隊公私協同合作，研究更安全的資料加密保存方法，並利用多雲備份與備援之架構，提升資料保存的安全性。

4. 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)均儲存及運作於本地端，如遭遇例如 DDoS 等重大網路資安攻擊事件時，官網服務可能因此遭受癱瘓，故急需要建置安全雲端鏈路及雲端架構，將業務資訊或個資較不具機敏性，以及與現有環境相依度不高的服務，逐年推動雲端化及雲端備份的機制，避免遭受重大網路攻擊或遭遇戰爭狀況時，導致相關資訊服務停擺。

5. 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，屬優先推動之單位，因此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多個關注面向，需

落實辦理資通系統等級所需之安全控制措施，爰此透過本計畫完善上述安全防護，以達成A級機關資通系統分級安全控制措施。

6. 本局為我國重要犯罪偵查與情報蒐集機關，為能提升本局第一線同仁科技偵查之能力，以因應科技快速變遷之新興犯罪態樣，方能降低人工查處之時間耗費，並有效打擊犯罪。此外近年來境外敵對勢力及有心人士，經常利用AI深偽技術，以及免洗式人頭帳號等科技犯罪手法，使司法人員在追溯爭議訊息的過程中遭遇諸多困難，因此須搭配先進之系統及分析工具，結合辦案思維進行深入剖析，以阻絕新型態及各種隱匿之異常社群行為手法或操作方式，故急需擴充原有設備功能(包含鑑識及相關軟硬體)並透過新型資訊科技進行分析，方能有效突破相關障礙以利偵辦犯罪案件。

7. 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年成長將近百分之四十，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，安排規劃基礎鑑識課程，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，透過完善分析搜扣案關資料，更有效率挖掘出線索及找出案件突破點。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。

8. 隨著網路與資訊設備的普及，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後，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，不易於當下迅速發現及阻止，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，因此需賡續充實科技設備，以強化資安調查能力及提升檢測效能。

貳、 實施策略及方法

1. 建構「多雲基礎建設」目標工作項目：

(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。

(2)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。

(3)建置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，同時連接加密系統確保資料安全。

(4)於異地機房部署相關網路監控及資安防護設備。

(5)核心服務於異地機房進行雙活平台建置與測試資料同步及規劃安排單一機房服務中斷時之切換演練。

(6)租賃合適之公有雲儲存空間,進行分持備份之加密碎片上傳至公有雲進行備份。

(7)強化核心服務於異地機房(含非核心服務遷移至公有雲)之多活平台及完成加密含金鑰管理規劃。

(8)滾動調整並完善公有雲與完整回復至地端之相關演練。

(9)因應資安攻擊及數位韌性之戰略需求，納入 DDoS 攻擊防護維運。

2.建構「資安戰略規劃」目標工作項目：

(1)將「行動調查既智慧分析系統」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)。

(2)導入「身分管理平台」及「單一簽入管理平台」，並擴大零信任架構驗證範圍，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。

(3)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，逐年將全機關使用者、設備及各系統均導入零信任架構。

(4)辦理網路跡證溯源系統更新及相關資料庫擴充。

(5)進行暗網犯罪情資搜尋系統軟體使用授權更新。

(6)擴增擴增資安誘捕防禦系統、資安維運自動響應功能及建置端點偵測及及應變機制，完成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。

(7)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。

3.建構「數位系統升級」目標工作項目：

(1)分年購置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。

(2)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。

(3)更新實驗室數據資料保存系統。

(4)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。

(5)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。

(6)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。

(7)持續導入導入「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」。

(8)透過 AI 相關技術以加值資料、持續導入基於 AI 技術之案件偵查分析功能及完成與整合所有開發功能

參、 計畫成本概估

1. 經費來源：中央政府總預算。
2. 計算基準：以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、臺灣銀行共同供應契約價計算。並循預算程序逐年編列，核定計畫總經費新臺幣 5 億 714 萬 7000 元，計畫期程：114 年至 117 年。

肆、 預期效益分析說明

本計畫係透過執行「多雲基礎建設、資安戰略規劃、數位系統升級」目標，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「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」，實踐「資安即國安」之戰略目標並強化本局數位韌性。預計完成目標效益：

1. 提升資訊機房可用性：目前僅有局本部資訊機房，最遲可於 24 小時內恢復運作，未來以新建備援機房因應緊急或災難停機，並規劃逐年縮短恢復時間，預期可於 4 小時工時內恢復運作。
2. 提升資訊服務數位韌性：逐年擴增多雲備份及備援節點數，預計 4 年內完成 3 座地端與 3 座雲端節點建置，並同時結合本局局本部資訊機房，共同有效提升數位韌性。
3. 完備統一驗證及授權機制：於計畫期程內，導入使用多因子認證及授權機制，並視業務及任務需求逐年提升使用率至 80%以上，以確保各項系統使用時之安全性。

4. 完備網路管理機制：藉由實施網路微分段、導流機制，搭配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，預計可逐年提升20%以上之防護效果。
5. 縮減資安事件預警時間及自動化處理人力：目前本局資安事件預警平均工時為 1.5 小時，自動化處理資安事件所需人力配置為 6 人，未來將逐年降低預警工時與所需人力配置，最佳可達到 30 分鐘內預警之工時，以及降低人力配置至 2 人。
6. 完成全球資訊網系統雲端移轉，同時建構全球資訊網系統承受 DDoS 之攻擊防護：目前本局全球資訊網並未建置 DDoS 攻擊防護機制，未來本計畫施行後，屆時將完善 DDoS 相關防護，將可更有效提升全球資訊網可用性與防護能力。
7. 提升網路跡證溯源系統利用頻度以及暗網資安情資內容可用度：透過以上系統之功能強化，提高情蒐效能與資料完整度，協助相關人員辦理上級交查任務及外勤處站進行轄區運用情資，於期程內將人員之系統使用度提升至 80%以上。
8. 增進鑑識人員專業能力：因應各項犯罪相關鑑識需求，業務量激增，本計畫預計提升取得資安鑑識相關專業證照，每年至少達三十人次以上，有效精進數位鑑識及現場取證量能。

9. 完成 API 管理服務平台、系統效能監控平台等各項建置：

目前本局並未建置以上相關平台，未來透過建置完成之平台，不論是新 API 服務提供率或者效能問題報告產出率，可望獲得有效提升，有助於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。

10. 行動調查暨智慧分析系統提供 AI 分析功能：目前本局尚未具備此功能，本計畫將逐年完成 AI 分析新功能建置，預計於 4 年內完成目標建置率，以期能更有效協助分析嫌犯個人基本資訊及與犯罪集團內成員關係。

伍、 結語

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，本計畫係以「多雲基礎建設」、「資安戰略規劃」及「數位升級」等 3 項主軸，同時導入雲端化、AI 等新興技術而建置維運相關系統，爰此由資通安全處統籌架構規劃、人力及經費籌用等事宜而擬定各項工作目標項目，以期達成數位韌性確保機關能及時應變各類風險。透過本計畫，建構嚴密之安全防護網，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，以維護國家穩定發展，謀求人民最高福祉。