「113 年度軍民通用資安技術研發補助計畫」公告事項

一、 計畫目標：

基於六大核心戰略產業之國防及戰略產業核心政策下，未來國防產業將朝向與民間資安自主研發能量結合之國防及戰略產業發展，為確保國防產業與相關基礎建設安全，本計畫藉由補助國內廠商業者，建立國內資安關鍵技術自主發展能量。

二、 補助範圍：

本計畫推動國內產業聚焦發展可建構台灣數位韌性之資安關鍵技術，以確保國防產業與相關基礎建設安全，並建立國內資安關鍵技術自主發展能量，本須知包含「一般型計畫」及「啟動型研究」2 類別，由企業自行擇定 1 個類別申請，須符合以下類別之一：

項目	一般型計畫（單獨/聯合）	啟動型研究（單獨）
主題類型	由企業選擇四大主題中的 1 個子類別進行申請，詳細內容請參考**四、徵案主題**。 (一)攻防演練平台： 1. 協作式紅隊平台 2. 演練式紅隊平台 3. 攻防腳本平台 4. 藍隊與紫隊演練平台 (二)供應鏈安全： 1. 晶片安全工具/技術 2. 設備安全工具/技術 3. 軟體安全、溯源管理工具/技術 4. 供應鏈安全工具/技術 (三)通訊與端點安全： 1. 元件與軟韌體安全 2. 通訊裝置與平台安全 3. 非同步衛星安全	符合軍民通用資安技術主題之新興產品技術研發。補助計畫從研究技術雛型發展成可展示驗證之雛型產品，需說明具備未來應用於解決國防、軍事相關領域挑戰議題之潛力，且提出產品技術研發路程與未來軍民通用場域驗證之規劃。

項目	一般型計畫（單獨/聯合）	啟動型研究（單獨）
	(四)新興資安技術： 1. 人工智慧（AI） 2. 零信任架構 3. 新興密碼技術 4. 其他	
補助經費	以新臺幣 1,000 萬元為上限	以新臺幣 350 萬元為上限
計畫期程	計畫公告日起至 114 年 1 月 31 日止	計畫公告日起至 113 年 7 月 31 日止

三、 審查重點（包含成效指標）：

重點項目	一般型計畫	啟動型研究
前期計畫執行成效與成果亮點	應具體描述前期計畫之執行成效與亮點、各項查核工作之符合情形、人力及經費運用情形、期中及期末審查建議改善情形。（若無前期計畫免填）	
計畫內容與軍民主題之扣合度	• 應具體描述本計畫整體架構與各工作項目與軍民主題之扣合度、適用之軍用情境、驗證場域、欲解決問題之痛點、開發與實施方式、技術規格與功能、測試驗證規劃做法、執行期程、查核指標、人力及經費、預期效益，以呈現整體計畫在國防或軍用領域應用之合理性、完整性及可行性。 • 若有前期計畫，則須補充說明前期計畫與本計畫之技術規格功能差異比較、技術深度或廣度延伸、本計畫執行重點及成效提升。	
技術優勢與競爭分析	應比較說明國內外主要競爭對手、所提研發標的之創新或關鍵之處、與競爭對手之規格功能差異比較、相對於競爭對手之優勢分析，及結合運用新興科技技術說明，如（但不限）人工智慧、機器學習、自動化機制等。	
自主研發能量與過去實績	應具體說明研發標的於開發完成前後，整體架構及各工作項目為自主研發、現有技術或基於現有技術進行研發之比例估算，說明如何達成技術自主化，並進一步說明申請業者過去之研發實績及執行能力，且不應使用或基於任何陸資產品或函式庫進行開發。	
資安研發能量	說明申請計畫之資安研發能量，如參與本計畫參與人員之資安證照情況、資安經費比例、本計畫欲提升資安研發能量之相關規劃等。	

重點項目	一般型計畫	啟動型研究
場域驗證（國防場域優先）	• 應具體說明研發標的於國內外軍工產業之潛力或預期合作對象，並說明做為合作夥伴或特定場域之前期關鍵技術研發，未來之技術發展方向與國內外市場佈局規劃。 • 若有前期計畫，則須說明研發標的於國內外軍工產業之合作對象（建議優先針對國防場域），並說明合作模式、市場布局及產業效益，並提供與國內外國防或軍工產業進行合作之佐證資料（如合作備忘錄、協議書）。	說明具備未來應用於解決國防、軍事相關領域挑戰議題之潛力，且提出產品技術研發路程與未來軍民通用場域驗證之規劃。
其他有利審查資料	1. 曾執行國防領域或與本計畫資安技術相關計畫之經驗與目標。 2. 補助範圍之資安關鍵技術，其衍生至國防、軍用產品開發或通過其他國際認驗證之規劃。 3. 具資安產品研發或執行國防相關專案、服務業務之實績說明。 4. 本案所研發之資安關鍵技術，與國內外國防或軍工產業進行合作之佐證資料（如合作備忘錄、協議書）。	

四、徵案主題：

(一)攻防演練平台

全面運用多種自動化攻擊與防禦手法，找出潛藏的漏洞進行攻擊並可進行有效阻擋。本主題除建立紅隊攻擊能量與藍隊防禦機制外，亦可將紅隊的攻擊方式與藍隊的聯防機制進行分享，建立紫隊之攻防策略規劃，此外，亦可納入模擬營運技術（OT）攻防演練場景項目，並發展雲端攻防演練平台與進行持續更新，及可支援現有常用平台運作之需求，藉以提升整體攻防演練平台之擬真度與全面性。

1. 協作式紅隊平台

研發具備多方協作與滲透測試功能之紅隊平台，並以進階持續性滲透攻擊（APT）為主，使攻擊者可藉由植入後門程式感染目標系統，並透過中繼站伺服器負責監聽之通訊協定，與後門程式溝通並監聽後門程式之

請求，達成攻擊、隱匿及規避之目的，並說明對應如：MITRE ATT&CK 的哪一個階段，以利識別與分析網路攻擊流程。本平台需可支援至少 100 位攻擊者使用 Client 端介面同時與中繼站伺服器進行連線與發送攻擊，其底層環境亦需能支援不同語言所開發的執行環境，並可儲存相關攻擊技術。

2. 演練式紅隊平台

研發可訓練紅隊成員具備紅隊攻防能力之演練式紅隊平台，使得紅隊成員可在受控環境中利用相關工具進行模擬攻擊，以便練習不同的攻擊技術與方法，本平台須具備可生成遠端主機控制程式、支援紅隊成員協同操作控制，以進行內網橫向移動測試之紅隊平台。平台之內部網路環境需設計切割為多個網段，至少需包含 DMZ 網段、OA 網段、IT 網段、核心系統網段，並且需於學員取得關鍵 flag 之後方得進入下一個網段進行相關攻擊之功能，並須支援 100 位以上訓練人員同時進行演練之需求。

3. 攻防腳本平台

研發與建立攻防腳本平台，蒐集與研析相關漏洞與駭客之入侵攻擊手法與流程，進而引導出自動化攻擊與防禦資訊，除剖析駭客攻擊手法外，亦可產出防護與修正對策與手段。本平台可具備正常行為網路流量的產生器或腳本之功能，並具備統一框架（如 Metasploit framework 格式），可上傳與儲存攻擊工具，並應涵蓋至少 100 個高風險弱點（須涵蓋至少近三年之高風險弱點），以利訓練識別正常及惡意的流量。

4. 藍隊與紫隊演練平台

研發負責抵擋外部攻擊或內部威脅之藍隊防禦技術，以保障組織內部機敏資訊安全與資通系統韌性。或結合紅隊的攻擊方式與藍隊的聯防機制，建立紫隊演練、合作、情資分享或訓練等機制或平台，並具備裁判的功能，以協助觀察、評估及自動化評分，俾利提升整體攻防演練平台之擬真度與全面性。

(二)供應鏈安全

發展可確保數位韌性相關場域（如非同步衛星與關鍵基礎設施等）安全之工具與技術，以評估整體供應鏈從晶片、設備、軟韌體，及暴露在外之資訊資產資安風險程度，並依照安全軟體開發生命週期，研發確保應用程式安全之安全軟體開發平台，以降低受攻擊之風險。

1. 晶片安全工具/技術

研發可確保晶片安全之工具/技術，包含（但不限）晶片保護與加解密技術、透過分析晶片在運行時之電壓、功耗、溫度、電磁、頻率等線索，

觀察可能從晶片洩漏之資訊，並利用相關方法論推測出明文、私鑰等機敏資訊之技術。

2. 設備安全工具/技術

研發可確保設備安全之工具/技術，包含（但不限）設備保護與實體安全技術、系統安全檢測技術（如韌體拆解與逆向工程）、身分鑑別與授權機制（如憑證偽冒與密碼破解）、韌體及實體入侵等檢測技術。

3. 軟體安全、溯源管理工具/技術

依照安全軟體開發生命週期（Secure Software Development Life Cycle, SSDLC），研發確保應用程式安全之安全軟體開發平台，本平台需可流程化管理與建置軟體開發專案威脅模型，制定 SSDLC 測試流程，並結合軟體供應鏈框架與清單，如軟體供應鏈安全框架（Supply chain Levels for Software Artifacts framework, SLSA）、軟體物料清單（Software Bill of Materials, SBOM）、漏洞可用性交換（Vulnerability Exploitability eXchange, VEX），產製可稽核之驗證表單。平台功能需可整合多元資安檢測、原始碼掃描、軟體物料清單、弱點資料庫等資安檢測與外部情蒐工具，建立應用程式開發過程中，弱點與漏洞之測試、追蹤、監控平台。

4. 供應鏈安全工具/技術

研發具備探析網路、網頁、網域、IP 位址、端點及應用程式安全等外部網路活動風險之自動化驗證工具，並利用 AI 模型/演算法對探析資料進行量測分析與分數評級，以評估廠商曝露在外與內部網路活動之資安風險程度。本自動化驗證工具需設定場域類別（如半導體、通訊、交通、金融、醫療等產業），並需有與實際場域驗測之實作經驗。

(三)通訊與端點安全

針對通訊系統或端點產品，研發元件、軟韌體、手持裝置、應用程式平台及可備援通訊之非同步衛星安全，確保系統透過安全通道進行通訊。

1. 元件與軟韌體安全

研發通訊系統或產品關鍵元件與軟韌體之資安技術，如加解密技術、身分認驗證技術、軟韌體安全更新技術、資料保護技術等。

2. 通訊裝置與平台安全

針對通訊裝置、行動應用程式或其他平台技術，利用輕量級通訊協定技術、安全介接技術通訊平台或應用程式認驗證技術等，強化通訊過程之資料傳輸安全或效能。研發單向閘道器以跨實體隔離網路達到安全傳輸數據。

3. 非同步衛星安全

針對非同步衛星（如低、中軌衛星）之「元件」、「通訊」、「操控」，研發關鍵元件、軟韌體、通訊平台、攻防漏洞認驗證之資安技術並進行場域實測。

(四)新興資安技術

運用新興科技技術，發展其他可強化國防與軍用領域之資安技術，並考量無法連線至網際網路進行更新、查詢或同步之因應方式。

1. 人工智慧（AI）

運用人工智慧相關技術，包含大數據分析、機器學習、深度學習、生成式人工智慧（Generative AI）及分辨式人工智慧（Discriminative AI）等，達成自動化處理資安事件，以降低人力成本並提高資安防護。

2. 零信任架構

基於零信任安全框架，研發如身分鑑別、設備鑑別及信任推斷或其他資安防護機制，以實現零信任架構之資安解決方案，有助於應對現代複雜的資安威脅環境。

3. 新興密碼技術

研發基於新興密碼技術以發展相關資安應用技術，如（但不限）後量子密碼學、量子密碼學。

4. 其他

研發其他有助於強化國防領域相關系統或設備之資安技術或工具。

五、 申請資格：

(一)國內依法登記成立之獨資、合夥、有限合夥事業或公司。

(二)非屬銀行拒絕往來戶，且公司淨值（股東權益）為正值。

(三)不得為陸資投資企業（依經濟部商業發展署商工登記資料公示查詢服務之股權狀況或經濟部投資審議司之陸資來臺投資事業名錄為準）。

(四)不得為本國設立及外國營利事業在臺設立之分公司。

六、 作業須知：

(一)補助案件之補助比例，不得超過申請補助計畫全案總經費之 50%，其餘經費由申請企業自籌。

(二)補助科目依「數位發展部協助產業創新活動補助獎勵及輔導辦法」公告項目。

(三)申請之企業應具備從事研究發展所需之人力與專案執行及管理能力，並有實際績效，足以進行申請計畫之產業技術研發。

(四)申請公司於 5 年內未曾有執行政府科技計畫之重大違約紀錄，及未有因執行

政府科技計畫受停權處分，且其期間尚未屆滿情事。

(五)同一企業或同一負責人於同一時期申請及執行之政府計畫總件數，不得超過3 件；但如為聯合提案企業（非主提案企業）、分包、委外廠商不在此限。若同一時期申請超過 1 個以上政府相關補助計畫，應於審查時主動說明企業資源配置分工；若曾執行過政府相關補助計畫，應說明該計畫成果及產業效益。

(六)計畫書應載明事項包括公司概況及經營團隊及執行能力、產業需求與挑戰、計畫目標與執行架構、計畫可行性分析等，申請計畫總期程一般型計畫自計畫公告日起至 114 年 1 月 31 日止，啟動型研究自計畫公告日起至 113 年 7 月 31 日止，申請之企業可提供完整計畫目標（2 年以上，不超過 3 年），並分年敘明應達成之重要里程碑與預期效益，以做為整體計畫審查或下一階段補助申請之參考。

(七)本計畫申請須知、經費編列範圍及計畫管理作業手冊等規範比照 DIGITAL+ 數位創新補助平台計畫規定辦理。

(八)為引導企業建立資安防護機制，以保障企業重要生產資訊，並提升企業資安防護能量，受補助企業應於**簽約前**完成「企業資安評級」（https://secpaas.org.tw/W_Menu_Service?ID=30）並檢附相關資料說明於計畫書中，且於計畫期末結案時再次更新，以了解企業資安能量是否持續提升。

(九)企業申請補助計畫之資訊安全項目經費應占總經費 7%以上，審查時應說明資安人力與資安委外所占比例，分別說明該案中之資安分工，對應解決的資安需求，資安委外包含的產品及服務內容，驗收時應提供支付資安廠商之給付證明、資安人力相關舉證資料（如，證照、論文、就業證明）等。

(十)申請計畫之團隊人員若提供具資安產品研發或執行國防相關專案、服務業務之實績說明尤佳。

七、 申請程序：

申請本專案計畫者，應於公告受理期間進行線上申請（網址：https://digiplus.adi.gov.tw，並須使用工商憑證），公告受理日期為自公告日起至 113 年 3 月 29 日（五）下午 5 時截止，恕不受理紙本送件，由本署籌組專業審查小組進行審查（專家小組得視需要至現場訪視），核定通過後簽約執行。

八、 其他注意事項

(一)本公告未盡事宜，應依「數位發展部協助產業創新活動補助獎勵及輔導辦法」及其他相關法令規定辦理。

(二)聯合申請的多家企業應互推 1 家主導，並共同簽訂「合作契約書」，並由全體參與企業高階主管成立管理委員會，協調處理有關整合及各企業間權利義務與爭議等事宜。

(三)主導企業及其餘參與企業皆須符合「五、申請資格」所列之規定。

(四)主導企業應具備研發管理之整合能力，有效處理多家企業共同執行計畫所產生之權利義務、任務分工、經費分配及計畫管理等有關事宜。

(五)申請應備資料：

1. 計畫申請表、申請公司基本資料表。
2. 所提計畫書之各項內容，須彙整全體企業之資料。
3. 申請企業（主導及聯合）均需繳交最近 1 年營利事業所得稅結算申報書（需包括損益及稅額計算表、資產負債表）。

(六)所有參與企業須派員出席審查會議及期中、期末查證會議，並須接受財務審查。

(七)審查通過之計畫，由主導企業與本署委託之機構簽約。執行企業應由管理委員會協調，提具簽約及請領補助款所應繳交之銀行履約保證金保證書。

(八)政府補助款由本部委託之機構撥付主導企業，再由主導企業撥付其他各執行企業，每家企業均須設立專戶儲存補助款。

(九)計畫執行期間，本部委託之機構得對執行計畫之全體企業進行查證作業，主導企業應負責彙整其他各執行企業之資料。

(十)依核准計畫進行之研發行為，如涉及公平交易法所稱之聯合行為，主導企業應另依規定向公平交易委員會申請許可。

(十一) 全體參與企業於計畫執行期間與結束後均應配合本署計畫成果展示宣導活動，並協助提供成果運用、投資金額、創造產值等計畫成效資料。