檔　　號：
保存年限：

數位發展部數位產業署　公告

發文日期：中華民國115年5月5日
發文字號：產服字第1156000265號

裝

訂

線

主旨：公告本署「DIGITAL+數位創新補助平台計畫」項下115年主題型計畫「軍民通用資安技術研發補助計畫」公告事項，自公告之日起正式受理申請。

依據：「數位發展部協助產業創新活動補助獎勵及輔導辦法」辦理。

公告事項：「軍民通用資安技術研發補助計畫」公告事項詳如附件。

署長林俊秀請假
副署長陳慧敏代行

115 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：

本計畫基於五大信賴產業方向進行推動，藉由補助國內業者，研發國防與軍用領域實際需求之資安關鍵技術，強化現有資通系統與資安防護機制，並協助民間提升技術能量，培養在地的業者，完備國內資安關鍵技術自主發展能量，促進軍方資安技術國產化。

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，並建立國內資安關鍵技術自主發展能量，本公告事項分為「一般型主題」及「國防需求主題」2 類別，由企業自行擇定 1 個類別申請，**補助範圍將優先補助「國防需求主題」類別**。

項目	一般型主題	國防需求主題
主題類型	由企業選擇四大主題中的 1 個項目進行申請，詳細內容請參考公告事項之**四、徵案主題(一)一般型主題**。 1. 攻防演練平台 1.1 協作式紅隊平台 1.2 演練式紅隊平台 1.3 攻防腳本平台 1.4 藍隊與紫隊演練平台 2. 供應鏈安全 2.1 晶片安全工具/技術 2.2 設備安全工具/技術 2.3 軟體安全、溯源管理工具/技術 2.4 供應鏈安全工具/技術 3. 通訊與端點安全 3.1 元件與軟韌體安全 3.2 通訊裝置與平台安全 3.3 非同步衛星安全 4. 新興資安技術 4.1 人工智慧（AI）	由企業選擇國防需求主題中的 1 個項目進行申請，詳細內容請參考公告事項之**四、徵案主題(二)國防需求主題**。 1. 攻防演練平台 1.1 工控數位孿生資安攻防演練模組 1.2 資安攻防演練場景藍圖自動產製模組 2. 供應鏈安全 2.1 AI 輔助晶片電路與軟韌體安全檢測技術 2.2 AI 輔助零組件供應鏈追溯與風險辨識技術 3. 通訊與端點安全 3.1 檔案共用監測系統 4. 新興資安技術 4.1 基於人工智慧之網路自主防禦系統 4.2 基於大型語言模型之語義

項目	一般型主題	國防需求主題
	4.2 零信任架構 4.3 新興密碼技術 4.4 其他	感知網際防禦閘道器研究計畫
補助經費	以新臺幣 1,000 萬元為上限	以新臺幣 1,200 萬元為上限
計畫期程	115 年 6 月 15 日起至 116 年 5 月 31 日止	

三、審查重點(包含成效指標)：

重點項目	一般型主題	國防需求主題
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	• 應具體描述本計畫整體架構與各工作項目、適用情境、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、通報的弱點數量、參與大型國際性或政府主導等攻防演練之經驗、參	

重點項目	一般型主題	國防需求主題
	與全球或國內的資安競賽且曾獲得獎項、具備資安相關的技術專利，以及曾經發表或受邀資安相關演說等。	
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）。	• 應依據國防提需單位之需求情境，說明研發成果未來於國防場域之驗證方式與應用規劃，並規劃場域驗證機制，以利評估研發成果於國防實務應用之可行性。
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或具列管軍品之合格認證。 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)一般型主題

1. 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。

1.1 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，及可具備自動滲透測試工具(模擬攻擊者行為，發現網路漏洞)及攻擊工具庫(內建 DDos、SQL 注入、XSS 等網路滲透工具)等模組。

1.2 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。

1.3 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，且可具備攻防場景、演練科目自動化生成功能，可快速產製攻防演練、系統驗測場景及演練科目，以降低演訓及測試規劃時間，與設定程序複雜度，並可依據演練科目變化程序，進行互動式交戰演練。

1.4 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。

2. 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。

2.1 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。

2.2 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。

2.3 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。

2.4 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。

3. 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。

3.1 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。

3.2 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、邊緣運算、網狀網路、分散式結構等技術等，強化通訊過程之資料傳輸安全或效能，並在網路大環境受限或受到資安威脅時維持裝置與平台的運行。例如可研發單向閘道器，具備資料傳輸審查機制，且傳輸紀錄須保存一年以上，並可支援多協定，如 UDP, TCP/IP, SFTP, NTP, SMTP 等，確保資料流動的單向性，以跨實體隔離網路達到安全傳輸數據。

3.3 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。

4. 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。

4.1 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。例如可智慧化針對日誌或網路流量進行關聯性分析，快速搜索異質設備的大數據情報，並比對分析出人工檢視難以察覺的潛在威脅及預警徵兆。

4.2 零信任架構

基於零信任安全框架，研發包括身分鑑別（如多因素驗證、行為分析）、設備鑑別（如設備指紋識別、端點安全狀態檢測）及信任推斷（如基於風險的存取控制、動態信任評分）等資安防護機制，並可整合如微分段、加密技術、威脅情報分享等先進技術，以實現全面且動態適應零信任架構的資安解決方案，以應對現代複雜多變的資安威脅環境，提升企業在應對內外部威脅時的防禦能力。

4.3 新興密碼技術

在現有密碼技術面臨量子計算威脅的背景下，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、全同態加密技術、區塊鏈與分散式密碼技術等，以強化系統安全性，並發展高效且具有可擴展性的資安解決方案。

4.4 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。

(二)國防需求主題

1. 攻防演練平台：

1.1 工控數位孿生資安攻防演練模組

(1) 預期效益：

A. 提供一套仿真工控設備模擬環境，具備虛擬數位孿生技術，可模擬工控設備之網路及控制行為。

B. 在通訊方面，支援多種工業通訊協定，能重現工控系統之通訊模式，以模擬實際工控環境之攻防演練情境。

C. 為提升可視性，提供圖形化介面，方便監控各節點的網路與控制行為，提升操作與分析效率。在設計上，採用模組化架構，並提供開放 API，允許擴充模擬環境或串接不同情境，以滿足多樣化之工控安全研究需求。

D. 此外，系統支援 MITRE ATT&CK for ICS 框架中的工控資安攻擊模擬，能夠更效驗證工控系統的防護能力與提供對應修改建議。

(2) 功能需求：

廠商需具備工業通訊協定分析模擬技術，並提供「數位孿生技術試研製軟體模組」，包含以下功能：

A. 發展工控設備數位孿生建模技術：可模擬 PLC、IED、SCADA 等設備之網路與控制行為。

B. 發展工業通訊協定模擬與分析技術：支援如 Modbus、IEC 61850 等通訊協定之行為重現。

C. 發展可視化監控與分析機制：呈現網路節點與控制行為，提升系統可觀測性。

D. 建立模組化架構與介面設計：支援系統擴充或不同場域情境整合之能力。

E. 發展工控資安攻擊模擬技術：參考 MITRE ATT&CK for ICS 框架，進行攻擊行為之模擬與驗證。

F. 進行應用場域驗證：如電力系統或智慧製造場域之攻防演練情境建置與測試。

G. 鼓勵結合實際工控設備特性（如國內外常見品牌）進行模型驗證，以提升擬真度。

H. 可針對特定場域（如 IEC 61850 電力系統）發展專用數位孿生環境與相關技術驗證。

I. 發展多樣化攻擊情境（如遠端連線、未授權控制、通訊攔截等）於數位孿生環境中之應用。

1.2 資安攻防演練場景藍圖自動產製模組

(1) 預期效益：

A. 自動產製攻防演練或系統驗測場景，減少人力參與程度。

B. 增加近年真實案例，掌握網攻趨勢。

(2) 功能需求：

廠商需具備 AI 生成、虛擬化平台等相關技術，並提供「場景自動生成工具」及「真實網路攻擊事件模擬場景」，包含以下功能：

A. 發展網路場域自動生成技術：透過自然語言或互動式方式，建立網路拓樸與系統架構。

B. 發展 AI 輔助場景建模技術：可協助定義節點類型（如主機、IoT、工控設備等）及其關聯。

C. 提供場景編修與調整能力：支援使用者對拓樸與節點參數進行調整與優化。

D. 發展結構化場景描述格式：支援如 JSON/XML 等格式，以利場景重用與系統整合。

E. 發展真實攻擊案例轉換技術：將近 1 年資安事件轉換為可模擬之攻防演練場景。

2. 供應鏈安全：

2.1 AI 輔助晶片電路與軟韌體安全檢測技術

(1) 預期效益：

A. 可針對具執行處理或儲存晶片(如無人機的飛行控制晶片、衛星定位晶片、通訊晶片等)及其軟韌體執行資訊安全檢測。

B. 導入 AI 輔助晶片電路與韌體安全檢測技術，將加速檢測時程與降低檢測成本，減少產品應用時的安全疑慮與資訊洩漏風險。

(2) 功能需求：

廠商需具備國際共同準則 (Common Criteria, CC)、物聯網安全評估標準 (SESIP)或美國聯邦資訊處理標準 (FIPS)等相關晶片安全檢測，韌體拆解與分析安全檢測及 AI 模型研發與驗證等技術或經驗，功能包含：

A. 發展晶片功能與安全行為分析技術（如通訊行為或識別機制）。

B. 發展 AI 輔助安全分析方法：應用於弱點偵測或旁通道攻擊分析等。

C. 建立晶片安全檢測流程或方法：包含旁通道攻擊相關檢測技術。

D. 發展韌體安全分析技術：包含韌體內容檢測與保護機制分析。

E. 建立韌體安全檢測流程與驗證方法。

F. 至少針對 1 類晶片應用（如通訊或無人機相關）進行技術實作與驗證。

2.2 AI 輔助零組件供應鏈追溯與風險辨識技術

(1) 預期效益：

A. 可有效提升偽造件識別率、來源透明度與資安防護能力，補足人工檢查的盲點與效率瓶頸，提升辨識效率與準確度。

B. 可自動完成 ICT 零組件盤點、標籤驗證、來源分析與異常偵測。

C. 可防止「偽造」、「高風險來源供應鏈」與具「資安風險」元件進入政府、國防、關鍵系統中，降低系統遭控制或資訊遭竊取風險。

(2) 功能需求：

廠商需具備影像與感測器工程、資料工程與資料集建置、AI 模型研發與驗證等技術或經驗，功能包含：

A. 建立電子零組件特徵與風險資料整合機制，作為 AI 分析基礎。

B. 發展資料庫擴充與整合技術：納入漏洞資訊（如 NVD）與供應鏈風險資料。

C. 發展 AI 輔助辨識技術：應用於真偽判別、來源分析與異常偵測。

D. 發展供應鏈檢測與分析模組：支援零組件風險評估與決策輔助。

3. 通訊與端點安全：

3.1 檔案共用監測系統

(1) 預期效益：

未來部署各營區，監測營區網路中檔案共用封包後，將告警資料回傳至中央監控系統，預估 14 個營區，可有效的監測內部網路

檔案共用服務傳輸資料內容，以防檔案洩漏。

(2) 功能需求：

廠商須具備廠商須具備網路封包側錄、協定解析、告警規則引擎、集中監控 Dashboard、身分驗證與日誌管理等技術能力，並提供一套「檔案共用監測系統」，包含以下功能：

A. 封包流量即時監控、SMB 及 FTP 封包分析。

B. 側錄封包結果可轉換為文字檔或 MNM/Wireshark/Malcolm 的資料格式。

C. Dashborad 顯示用戶單位、帳號(AD)、網卡號碼、來源、目的 IP 位址、傳輸檔案名稱或內容等基本資訊。

D. 使用者可以定義關鍵特徵碼，讓系統自動告警。

E. 裝置、使用者皆須身分驗證(零信任機制)。

F. 系統日誌不得儲存於公開網路或第三方平台。

G. 管理介面需角色分級及多因子驗證。

H. 執行日誌集中管理、設備狀態監控(含異常告警)及流量統計功能，系統日誌保存達 1 年以上。

4. 新興資安技術：

4.1 基於人工智慧之網路自主防禦系統

(1) 預期效益：

A. 縮短反應窗口：將防禦響應時間從數日縮短至分鐘級，反制 AI 武器的飽和攻擊。

B. 填補人力缺口：以 AI 代理人取代昂貴的人工紅隊，降低演練成本並提升演訓頻率。

(2) 功能需求：

廠商需具備AI紅隊、自動化攻擊編排、多代理人協作與地端LLM部署等相關技術，並提供「可用 HexStike-AI(或 NeuroSploitv2)組建工具組建之地端 LLM 自主攻擊紅隊模型」乙式，包含以下功能：

A. 地端 LLM 紅隊模型：可於國軍封閉式內網環境運行，具備超越傳統腳本，可意圖驅動之自主滲透能力，並能進行弱點探測、攻擊路徑規劃與行動執行。

B. 多代理人協作架構：須具備多代理人協作機制，可透過 MCP 協定或等效機制整合至少 150 種攻防工具，並具備即時決策支援。

4.2 基於大型語言模型之語義感知網際防禦閘道器研究計畫

(1) 預期效益：

A. 反制 AI 攻擊工具：有效阻斷如 HexStrike-AI 與 Cyberspike's Villager 等自動化攻擊框架的滲透行為縮短軟體修補時間窗口，在原廠釋出安全修補程式前，防火牆能根據漏洞描述自動生成語義過濾規則，達成「虛擬修補」效果。

B. 低誤判率：透過 LLM 理解上下文脈絡，減少傳統防火牆因過度防禦而產生的誤報，確保指管系統順暢運作。

(2) 功能需求：

廠商需具備網路封包解碼、入侵偵測/防禦、LLM 地端推理與加速、規則生成與沙箱驗證等相關技術，並提供「具 HexStike-AI(或 NeuroSploitv2)之地端 LLM 模型」乙式，包含以下功能：

A. 封包語義化與行為推理：可將底層網路流量進行解碼與特徵抽取，並利用地端微型 LLM 進行威脅建模與行為語義推理，將封包/連線轉換成可判讀之行為語義與攻擊意圖表示。

B. 自動規則生成與沙箱驗證：具備自動生成防火牆規則、WAF/IPS/IDS 規則或防禦腳本之能力，並能於沙箱環境預先驗證規則有效性與安全性，避免對正常流量造成破壞後才上線。

C. 高效能推論加速與即時處理：針對網路存取即時性需求，需優化 LLM 推論速度與吞吐量（含推論加速設計），系統應可支援至少 1Gbps 以上之網路流量處理能力，能支援作戰單位網段實際串接運作。

五、計畫時程

執行期程自 115 年 6 月 15 日起至 116 年 5 月 31 日止。

六、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（權益總計或權益總額）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。

(五)參與本計畫人力不得為大陸地區人民。

七、作業須知：

(一)國防需求主題之補助經費以新臺幣 1,200 萬元為上限，一般型主題之補助經費上限為新臺幣 1,000 萬元，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，申請計畫總期程自 115 年 6 月 15 日起至 116 年 5 月 31 日，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**申請時**完成 171 題「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115年6月12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本票及銀行履約保證金保證書。

(八)政府補助款由本署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，本署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。

(十二) 為避免研發成果等機敏資料遭不當竊取而致資訊外洩，投入本計畫之研發人員不得為大陸地區人民；所使用之資通訊產品（含硬體、軟體及服務）不得採用中國大陸廠牌產品。另資通訊產品及雲端服務不得涉及中國大陸（含香港、澳門）來源、IP 連線，或資料存取、備份、備援及跨境傳輸等情形。

(十三) 為確保國家安全及資訊安全，如屬經濟部投資審議司公告之「具敏感性或涉及國家安全（含資安）疑慮之業務範疇」，應排除陸資企業參與。