數位發展部
Ministry of Digital Affairs

# DIGITAL+數位創新補助平台計畫

## 主題型計畫
## 軍民通用資安技術研發補助計畫

## 徵案宣導說明會

日期：112年4月21日

數位發展部 數位產業署
Administration for
Digital Industries,
Ministry of Digital Affairs

壹

# DIGITAL+數位創新補助平台
# 申請辦法及補助機制

DIGITAL+計畫執行單位

財團法人台灣中小企業聯合輔導基金會

# 一、計畫依據

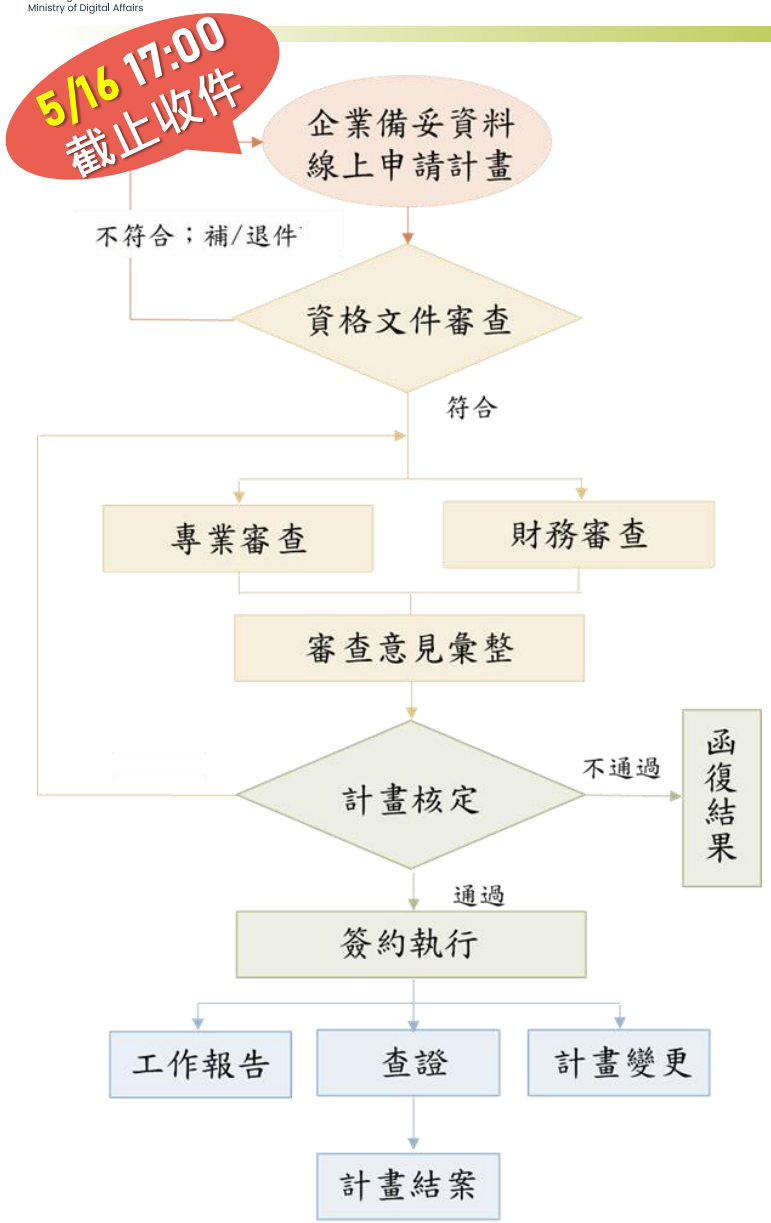
扣合「**數位國家、創新經濟發展方案**」的政策綱領，為本署達「**數位產業化、產業數位化**」之施政重點，透過獎補助機制扶植數位相關產業，建構有利數位創新發展環境，持續提升各項基礎建設，透過獎勵及補助機制帶動產業自主研發能量，以實現「**建構全民數位韌性**」、「**產業數位轉型**」之政策目標。

| | |
|---|---|
| **遠景** | **數位國家、智慧島嶼** |
| **政策依據** | **5+2產業創新**：亞洲矽谷、生醫產業、國防產業、智慧機械、綠能科技、新農業、循環經濟<br>**六大核心戰略產業**：資訊及數位、資安卓越、精準健康、民生及戰備、綠電及再生能源、國防及戰略 |
| **推動策略** | 研發獎勵/補助計畫 ⋙ 厚植數位產業研發能量、揚升數位創新應用價值<br>建立各行各業數位韌性、加速數位轉型提升競爭力 |
| **施政目標** | **推動產業創新數位轉型**、**淨零碳排**、**能資源永續管理**、拓展經貿布局、擴大投資臺灣 |

# 二、計畫架構與推動作法

| 計畫類型 | 數位新創應用獎勵計畫 Digistar<br>獎新創 | 數位服務創新補助計畫<br>補創新 | 主題型計畫<br>推主題 |
|---|---|---|---|
| 形式 | 獎勵 | 補助 | 獎勵或補助 |
| 說明 | 獎勵表揚已有初步市場落地實績與具備高成長潛力之軟體與資訊服務相關新創企業 | 透過研發補助方式，鼓勵軟體與資訊服務企業開發具共通性、關鍵性之前瞻數位技術開發，或具市場應用價值或社會公益之數位創新解決方案 | 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 |
| 組別/領域 | 產業加值、商務應用、高齡社會、淨零碳排、其他數位創新 | POC→POS：前瞻技術開發、<br>POS→POB：企業營運應用、終端消費應用、永續社會應用 | 紅隊攻防演練平台<br>供應鏈安全<br>非同步衛星安全 |
| 獎/補助經費 | 100萬 /家 | 1,500萬上限/案<br>(補助比例50%以下) | 1,000萬上限/案<br>(補助比例50%以下) |
| 期程規劃 | - | 執行期間不超過2年 | 執行期間不超過1年 |

# 三、計畫作業流程與時程




## 一、申請階段

- 於5/16下午5點前完成申請。

## 二、審查階段

- 資格審查：申請單位資格確認及應備資料完整性資料缺漏可補正者，應於計畫執行單位通知期限內完成補件。
- 財務審查：聯輔基金會查核企業及負責人票據信用、存款實績及往來情形。
- 書面審查：審查委員審查計畫書內容並提供審查意見。
- 會議審查：由計畫主持人進行簡報提案說明。

## 三、核定與簽約

- 函知審查結果（通過/不通過）。
- 核定通過之企業依核定函修正計畫書並進行複閱程序，並於時限內辦理簽約；完成簽約後依規定請領第一期補助款。

## 四、執行與結案

- 於計畫期程（112年11月30日）結束前安排結案審查。
- 依補助款請領方式安排財務查核。

# 四、計畫可編列之經費項目

3.設備使用費項下
【頻寬費】、【雲端設備租賃費】
執行專案於計畫期間內新增且僅供專案使用之頻寬及雲端平台及運算設備。

5.無形資產之引進、委託研究或驗證費

- 資安經費-申請補助計畫之資訊安全項目經費應占總經費7%以上，提案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。
- 驗證費-專為執行開發計畫所需，申請企業得將驗證場域企業之費用編列於委託研究項目內，惟本項經費編列以不超過計畫總經費比例10%為原則，然資安經費需達7%之規定不在此限。

6.國內差旅費

- 專為執行開發計畫所需並於計畫執行期間內，創新或研究發展人員往返核准場域所生之國內差旅費。

7.創新服務推廣費

- 專為執行開發計畫所做之推廣活動，以不超過計畫總經費比例10%為原則。

8.專利申請費

- 專為執行開發計畫於計畫執行期間內提出申請，國內專利3萬元、國外10萬元，經費科目不得變更。

金額單位：千元

| 會計科目 | 補助款 | 自籌款 | 合計 | % |
|---|---|---|---|---|
| 1.創新或研究發展人員之人事費 | | | | |
| （1）創新或研究發展人員 | 0 | 0 | 0 | % |
| （2）顧問、專家費 | 0 | 0 | 0 | % |
| 小計 | 0 | 0 | 0 | % |
| 2.消耗性器材及原材料費 | 0 | 0 | 0 | % |
| 3.創新或研究發展設備使用費 | 0 | 0 | 0 | % |
| 4.創新或研究發展設備維護費 | 0 | 0 | 0 | % |
| 5.無形資產之引進、委託研究或驗證費 | | | | |
| （1）無形資產引進費 | 0 | 0 | 0 | % |
| （2）驗證費 | 0 | 0 | 0 | % |
| 小計 | 0 | 0 | 0 | % |
| 6.國內差旅費 | 0 | 0 | 0 | % |
| 7.創新服務推廣費 | 0 | 0 | 0 | % |
| 8.專利申請費 | 0 | 0 | 0 | % |
| 開發總經費 | 0 | 0 | 0 | - |
| 百分比 | % | % | % | 100% |

計畫補助款不得超過
計畫總經費之50%

# 五、計畫申請注意事項(1/3)

## ◆申請資格：

本計畫應由1家業者（主提案業者）提案，相關業者應符合以下資格：

1. 申請企業為國內依法登記成立之獨資、合夥、有限合夥事業或公司，且研發標的須為自行研發之產品、技術或服務，不得僅為經銷、代理或代購。

2. 申請企業均非屬銀行拒絕往來戶，且公司淨值（股東權益）為正值。

3. 所有參與計畫之企業，不得為陸資投資企業（依經濟部商業司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委員會之陸資來臺投資事業名錄為準。）

4. 申請企業不得為本國設立或外國營利事業在臺設立之分公司。

# 五、計畫申請注意事項(2/3)

- 計畫為線上申請，需使用工商憑證申請帳號後，方可登入進行申請資料填寫。
- 補助計畫時程至1年為限。
- 本主題型計畫補助經費以新臺幣1,000萬元為限，且補助經費不得超過計畫總經費之50%。
- 需聲明符合下列條件，倘經舉報或查證與事實不符者，本署得駁回申請或撤銷補助資格：
  1. 本次申請計畫內容，未曾獲其他政府計畫補助者（包含已接受其他計畫分包/委外）。
  2. 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。
  3. 於3年內執行本署之研發補助計畫件數不得超過2件。
  4. 申請標的不得為已開發之技術或服務者。
- 計畫經費僅限於研發所需經費，區分為補助款與自籌款兩項，均列入財務查核範圍。
- 計畫經費之編列應與公司近3年相關研究發展經費相當或與營業額比例合理。

# 五、計畫申請注意事項(3/3)

申請應備文件

| | | |
|---|---|---|
| 01 | **DIGITAL+數位創新補助平台計畫申請表暨企業聲明/同意書** | **線上填寫** |
| 02 | 會計師簽證之財務查核報告書；若無會計師簽證之財務查核報告書，請上傳近3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）。 | 需有會計師簽章、公司大小章 |
| 03 | 企業申請計畫之個資同意書 | 本人親簽 |
| 04 | 徵信查詢同意書 | 公司大小章、負責人章 |
| 05 | 計畫書及相關附件 | PDF檔案上傳 |
| 06 | 驗證場域/業者合作意向書（雙方用印） | 隨計畫書檢附 |
| 07 | 委外單位合作意向書（雙方用印） | 隨計畫書檢附 |

# 六、計畫書撰寫注意事項(1/4)

## 計畫摘要表（續）

計畫摘要

一、 公司簡介
（一）公司名稱：
（二）核准設立日期： 年 月 日
（三）負責人：
（四）主要營業項目：

二、 目標市場需求分析

三、 目標市場業者痛點分析

四、 預計產品開發與技術或服務說明

五、 計畫執行優勢

六、 計畫結案後 3 年內預期效益

N是結案年

1

單位：千元

| | 計畫效益 | 項　目 | N+1 年 | N+2年 | N+3年 |
|---|---|---|---|---|---|
| 量化效益 | 經濟效益 | 計畫產出項目數（如：技術/產品/服務等項目數） | | | |
| | | 計畫成果銷售量（件） | | | |
| | | 計畫成果銷售額（千元） | | | |
| | | 計畫衍生投資額（千元） | | | |
| | 創新效益 | 專利申請（件） | | | |
| | | 專利核准（件） | | | |
| | | 研究產出（如：數位技術/軟體開發/產業應用 等研究報告件/篇數） | | | |
| | 社會效益 | 增加就業（人數） | | | |
| | | 研發人才培育（人數） | | | |
| | | 建教合作學校數（所）/人數 | | | |
| | 學術成就 | 學術活動（場） | | | |
| | | 學術發表（篇） | | | |
| 質化效益 | | | | | |

七、 計畫關鍵字：（請至少列出三項）

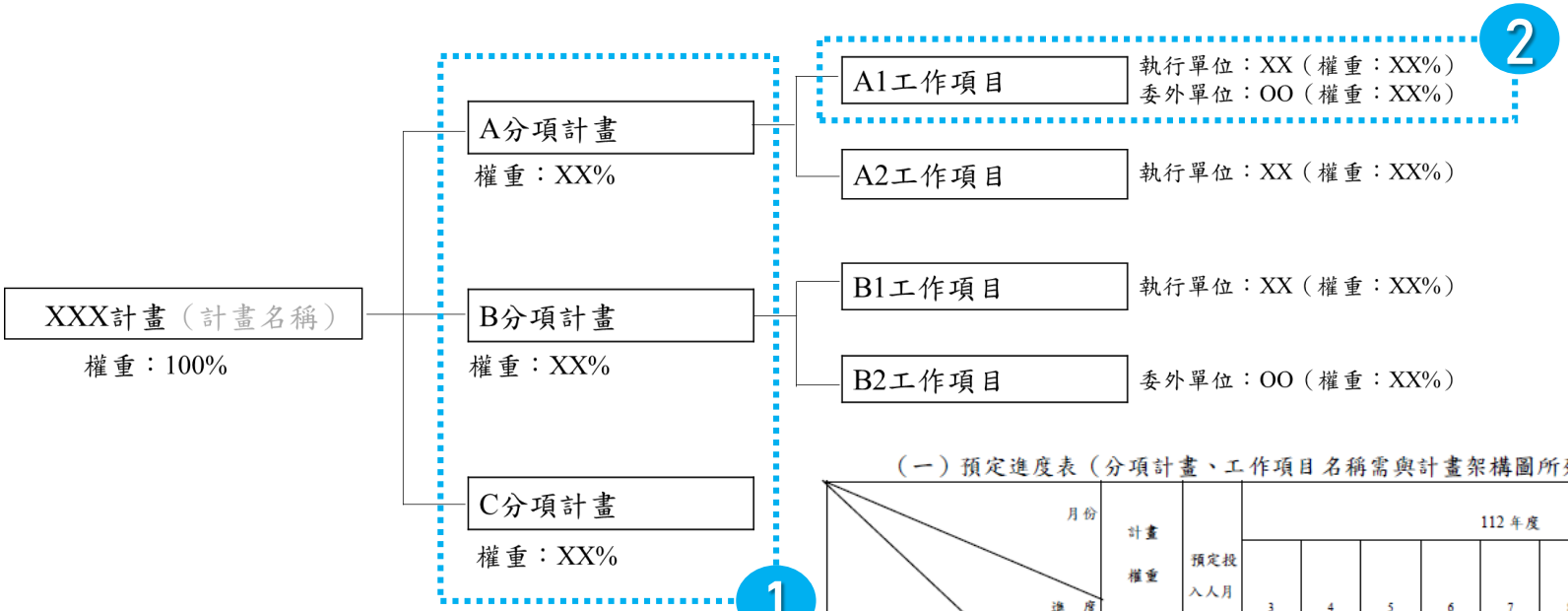
## 計畫書目錄



2 計畫書編列頁碼起始頁是目錄頁

1

# 六、計畫書撰寫注意事項(2/4)




（一）預定進度表（分項計畫、工作項目名稱需與計畫架構圖所列名稱及權重一致）

| 工作項目 / 月份 / 進度 | 計畫權重 % | 預定投入人月 | 112年度 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| A.XX分項計畫 | | | | | | | | | | | |
| 1.工作項目 | | | A1 | | | A2 | | | A3 | | |
| 2.工作項目 | | | | | | | | | | | A4 |
| 3.工作項目 | | | | | | | | | | | |
| B.XX分項計畫 | | | | | | | | | | | |
| 1.工作項目 | | | | | | | | | B1 | | B2 |
| 2.工作項目 | | | | | | | | | | | |
| C.XX分項計畫 | | | | | | | | | | | |
| 1.工作項目 | | | | | | C1 | | | C2 | | C3 |
| 2.工作項目 | | | | | | | | | | | |
| D.XX分項計畫 | | | | | | | | | | | |
| 1.工作項目（無形資產引進/委託研究/驗證：XX單位） | | | | | | | | | | D1 | |
| 小計 | 100% | | | | | | | | | | |
| 進度百分比% | | | % | % | % | % | % | % | % | % | % |

1) 計畫書資料前後應一致，如：分項計畫名稱、工作項目內容、工作項目權重占比。
2) 計畫架構圖各工作項目應敘明執行單位及委外單位分別負責之工作權重。

# 六、計畫書撰寫注意事項(3/4)

1. **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，請進行資安說明。（須符合本計畫之資訊安全要求，倘有開發或對外提供服務之行動應用App，亦須符合行動應用App基本資安規範）**
2. 請敘明是由企業自辦或委外，並將各經費中與資訊安全相關項目經費**分項列出，並計算資安經費總額**：○○○千元（佔總經費○%）。

| 會計科目 | 資訊安全項目 | 內容說明 | 適用人力、設備與系統<br>（參與計畫人力、應用程式、IoT 閘道器、網路、後臺伺服器、應用程式或其他） | 資訊安全經費（千元） |
|---|---|---|---|---|
| (範例)驗證費 | 資訊安全認證 | 資訊安全驗證評估報告 | 場域驗證 | |
| (範例)創新或研究發展人員之人事費 | 系統開發、規畫建置之工程與管理人員 | 伺服器、網路資訊安全維護 | 後臺伺服器、網路建置（工作項目） | |
| 資訊安全經費合計=（A） | | | | |
| 計畫總經費（自籌款+補助款）=（B） | | | | |
| 資訊安全經費佔總經費之比率＝（A）/（B） | | | | |

# 六、計畫書撰寫注意事項(4/4)

（一）預定進度表（分項計畫、工作項目名稱需與計畫架構圖所列名稱及權重一致）

| 工作項目 \ 月份 / 進度 | 計畫權重 % | 預定投入人月 | 112年度 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| A.XX分項計畫 | | | | | | | | | | | |
| 1.工作項目 | | | A1 | | | A2 | | | A3 | | |
| 2.工作項目 | | | | | | | | | | | A4 |
| 3.工作項目 | | | | | | | | | | | |
| B.XX分項計畫 | | | | | | | | | | | |
| 1.工作項目 | | | | | | | | | B1 | | B2 |
| 2.工作項目 | | | | | | | | | | | |
| C.XX分項計畫 | | | | | | | | | | | |
| 1.工作項目 | | | | | | C1 | | | C2 | | C3 |
| 2.工作項目 | | | | | | | | | | | |
| XX分項計畫 | | | | | | | | | | | |
| 1.工作項目（無形資產引進/委託研究/驗證：XX單位） | | | | | | | | | | D1 | |
| 小計 | 100% | | | | | | | | | | |
| 進度百分比% | | | % | % | % | % | % | % | % | % | % |

（二）預定查核點說明

| 查核點編號 | 預定完成時間 | 查核點內容 | 參與人員編號 |
|---|---|---|---|
| A1 | 112/03 | | |
| A2 | 112/06 | | |
| C1 | 112/06 | | |

① 年度別請以會計年度填寫，各分項計畫每季至少應有一項查核點，內容並應具體明確。

② 依各分項計畫之工作項目順序填註，分項計畫與本案研發組織及人力應相對應（不含聘任顧問、專家）

③ 查核點應按時間先後再依計畫順序依序填註，查核內容應係具體完成事項且可評估分析者，產出物並應有具體指標及規格且可量化，宜避免以「報告、手冊、圖、百分比等」概括，以利計畫執行成果驗收。

④ 無形資產引進/委託研究/驗證之工作項目，工作進度列入查核點，但人力則不編入投入人月。

# 七、其他提醒事項

1) 計畫主持人應為主導公司具營運決策權之專任人員，且須於審查會議到場簡報。
2) 申請遞件時應備妥無形資產引進/委託研究/驗證之合作意向書，俟核定通過後，須提供正式簽署之合約書影本。
3) 各項表格填列，倘無資料，請填「0」或「 - 」。
4) 計畫申請資料避免前後不一致，如：
   - 計畫書申請表、計畫書摘要表、開發總經費預算表、3.1年度經費使用分配表及各項經費編列表（表2.1-表2.8）金額需一致（含四捨五入及小數點）。
   - 計畫書摘要表、計畫預定進度表、參與計畫人員簡歷表、人事費表2.1（不含顧問人月數）之人月數須一致。
   - 計畫架構圖、分項計畫說明、預定進度表之各分項計畫與工作項目內容（文字說明、執行單位/無形資產引進(技轉)單位/委外單位/驗證單位名稱、各相應權重）均須一致。
5) 計畫送件請提早完成工商憑證元件安裝後點選送出，於收到「案件申請成功通知信」，才算完成送件程序。

貳

# DIGITAL+數位創新補助平台
# 提案方向與審查重點

輔導諮詢團隊
工業技術研究院 資訊與通訊研究所

# 計畫目標

## 資安技術 自主研發

本計畫藉由**補助國內資安業者**，深化國內資安關鍵技術，強化自主研發能量，確保國防產業與相關基礎建設安全，保護未來國防及戰略產業發展。

## 場域實證 國造國用

推動產業投入軍民通用資安產品技術研發，辦理國防單位**需求媒合**，進行軍民互用**場域實證並審查**，以落實自主資安關鍵技術國造國用。


本計畫基於六大核心戰略產業之「國防及戰略」、「資安卓越」策略方向發展。

# 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，補助範圍包含「紅隊攻防演練平台」、「供應鏈安全」、「非同步衛星安全」三大主題。

# 紅隊攻防演練平台

**全面運用多種自動化攻擊手法，測試目標系統弱點，找出潛藏漏洞並進行攻擊，本平台亦提供訓練紅隊成員之機會，包含模擬攻擊、分析漏洞以及訓練使用各種工具與技術來實現攻擊。**

- **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50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。
- **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。
- **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。本平台需具備統一框架（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）。
- **其他**
  - 研發其他有助於發展攻擊或培訓抵禦內外部資安威脅之網路攻防技術或工具。

# 供應鏈安全

**發展可維持數位韌性相關場域（如非同步衛星與關鍵基礎設施等）之「晶片安全檢測工具/技術」、「設備安全檢測工具/技術」、「軟體安全、溯源管理工具/技術」及「供應鏈安全檢測工具/技術」等，以評估廠商暴露在外之資安風險程度，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。**

- **晶片安全檢測工具/技術**
  - 研發可檢測晶片是否具備抵禦入侵與偵測入侵之能力，相關技術如透過（但不限）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。
- **設備安全檢測工具/技術**
  - 研發針對設備安全之檢測工具，包含（但不限）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）、通訊安全檢測技術、韌體及實體入侵等檢測技術。
- **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。
- **供應鏈安全檢測工具/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。
- **其他**
  - 研發其他有助於提升整體供應鏈安全之資安產品解決方案、技術或工具。

# 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。**

- **元件與軟韌體安全**
  - 研發非同步衛星關鍵元件與軟韌體之資安技術，如衛星晶片安全、加解密技術、身分認驗證技術、軟韌體安全更新技術等。
- **手持裝置與平台安全**
  - 研發非同步衛星通訊與平台之資安技術，如適用於衛星通訊之輕量級通訊協定、衛星通訊或廣播安全存取技術、衛星通信抗干擾及安全介接技術、衛星通訊平台或應用程式認驗證技術，其接收設備包含地面終端站台或手持裝置，於地面終端站台則需提供加密機制或保密防護之設計。
- **攻防漏洞認驗證**
  - 透過現有資安技術，研發適用於衛星系統之資安攻防與漏洞檢測技術，如衛星與虛擬基準站漏洞與安全（通訊、定位、廣播及導航等）檢測技術、衛星軟硬體漏洞掃描技術、衛星反監聽或惡意程式反組譯工具、衛星紅隊工具開發等。
- **其他**
  - 研發其他有助於強化非同步衛星安全之資安技術或工具。

# 審查重點與配合事項

- 申請廠商須依據下述審查重點，進行計畫申請撰寫之規劃
  - (一) 計畫內容與軍民主題之扣合度
  - (二) 技術優勢與競爭分析
  - (三) 自主研發能量與過去實績
  - (四) 國內外潛力軍工產業合作夥伴與市場佈局規劃
- 配合事項
  - 企業資安評級
  - 資安廠商聯合提案
  - 成果展示宣傳
- 其他

# 審查重點1：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。

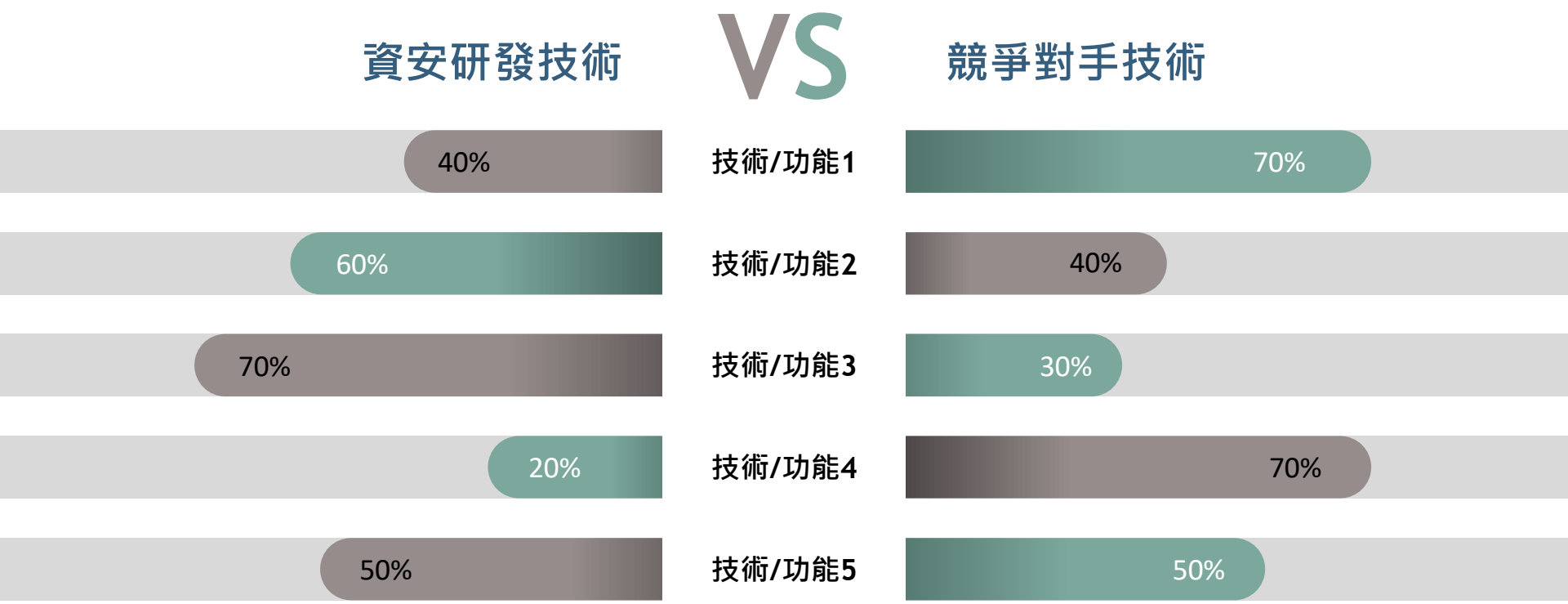
定義痛點與需求
(要解決軍用的什麼問題?)

重點關注項目與發展目標
(國際趨勢、新興科技)

資安技術研發

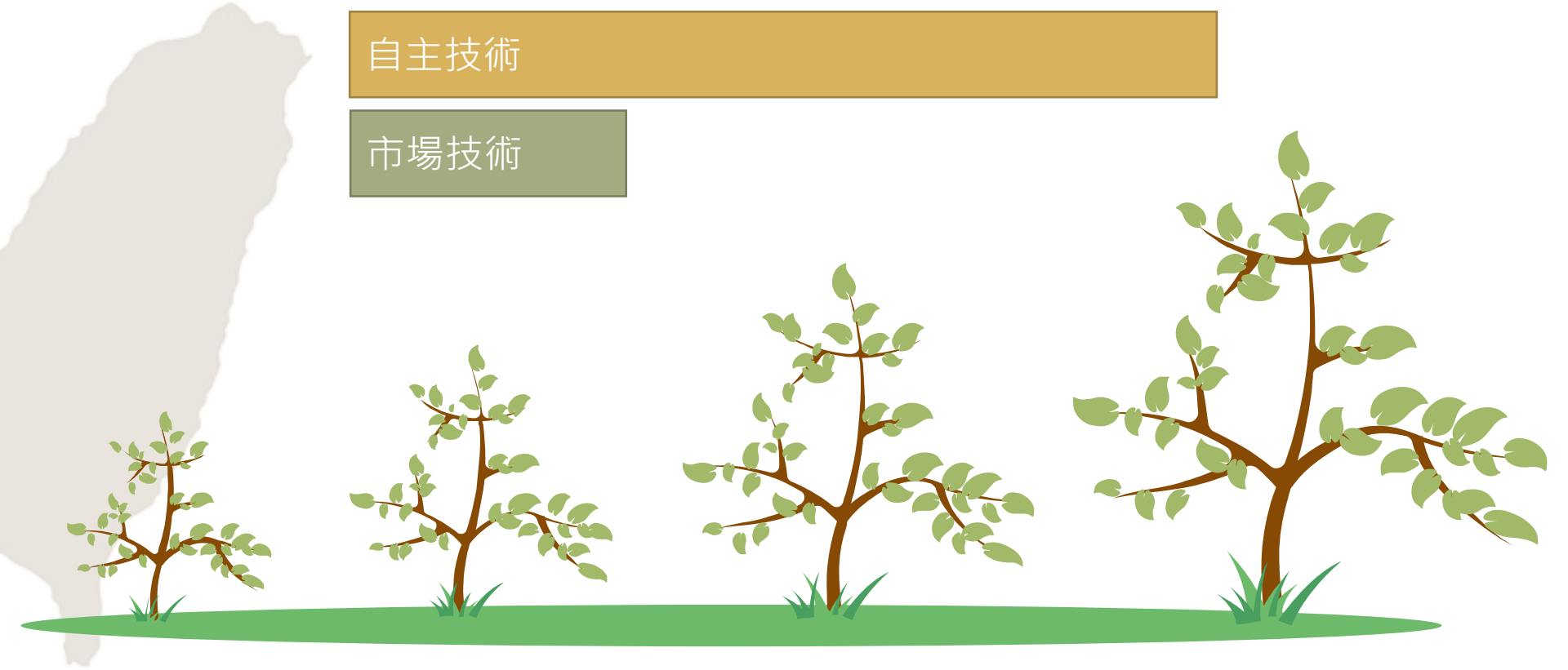
# 審查重點2：技術優勢與競爭分析

- 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。



# 審查重點3：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。

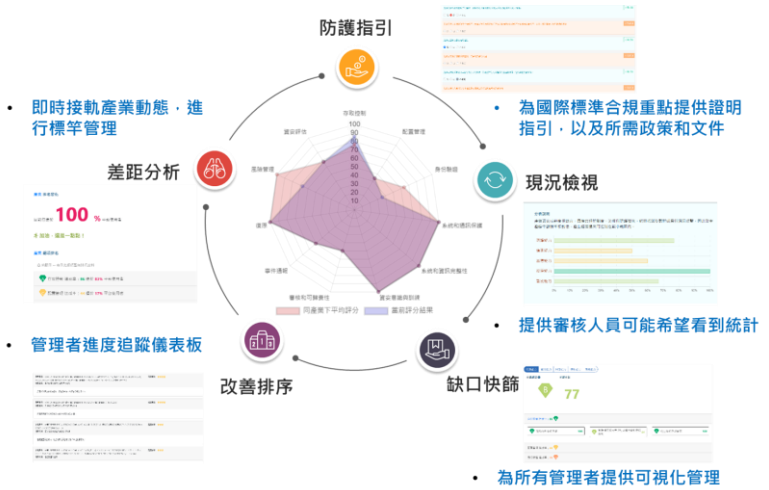


# 審查重點4：國內外潛力軍工產業合作夥伴與市場佈局規劃

- 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。

# 配合事項

- 企業資安評級
  - 配合數位部產業署新興物聯網資安示範推動計畫所推動之企業資安評級服務，進行企業整體資安風險評估，深度了解並釐清企業自身資安痛點。
  - 計畫申請前
    - 完成企業資安評級服務自評(完整版171題)（https://ratings.secpaas.org.tw/）。
    - 了解與釐清企業自身資安痛點，於提案時根據資安成熟度評估結果規劃資安升級作法。
  - 計畫執行期間
    - 持續更新企業資安評級服務。
    - 配合期中與期末查訪，提供查驗資料證明資安持續提升。




- 資安廠商聯合提案
  - 申請計畫之團隊若非資安廠商，則於申請提案時須與資安廠商聯合進行提案。
- 成果展示宣傳
  - 於計畫結束後均應配合本部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。

# 其他

- 計畫可行性
  - 計畫書完整性、可行性、經費編列合理性、團隊組成與執行經驗等。
  - 本計畫補助時程以1年為限，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。
- 其他有利審查
  - 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。
  - 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。
  - 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。

# 計畫諮詢

- 相關申請方式請詳閱計畫網站(申請須知下載)
  - https://digiplus.adi.gov.tw/plan_detail_5.html

- 計畫諮詢專線
  - （02）2396-6070

按讚、加入粉絲專頁

# JOIN ADI FB !

掃描 QR CODE

數位發展部數位產業署

# 感 謝 您 的 聆 聽

Thank You

DIGITAL+
數位創新補助平台計畫

（02）2396-6070
https://digiplus.adi.gov.tw/

# 交流與討論

數位發展部 數位產業署
Administration for
Digital Industries, moda