科技部「資安前瞻創新研發專案計畫」徵求公告

壹、宗旨

本部為配合政府施政藍圖以及行政院國家科學技術發展基金管理會補助「跨部會署科技計畫」規定，辦理推動五大創新產業(包括：綠能、國防、智慧機械、生技醫藥、亞洲矽谷等)之國防(資安)項目，帶動台灣經濟邁向創新驅動發展模式，並依據「106 年度推動創新產業研發補助旗艦計畫作業準則」規定，規劃推動本「資安前瞻創新研發計畫」。本計畫以產業需求導向（end-point）擬定國內急需研發之資安技術缺口，從上而下（top-down）推動相關前瞻研究領域發展，並加強產官學研資安研究鏈結，因此本計畫著重產業需求及具前瞻性的資訊安全研究項目，期與國際資安技術接軌。

貳、專案研發重點

本專案重點推動之研發主題與文件格式請參考**附件**說明。

一、 專案要點

(一)主持人需依本司規定之作業流程執行計畫、繳交各項文件電子檔、參與各項相關活動。期末必須提出完整的測試報告電子檔，於成果發表會向審查委員說明，必要時將進一步安排審查委員到計畫執行單位進行現場訪視。

(二)計畫績效評估指標：**本專案重視研發成果之創新應用效益及後續擴散效益**，計畫申請審查及成果審查時，將落實下列績效指標之評估，並做為科技部後續計畫核定之重要依據（以當年計畫成果或本專案補助之前期計畫成果為基準）：

1. 技術前瞻、創新應用服務範圍、運用成效等。請說明技術或應用創新的重點及與計畫推動構想的關聯性，亦請說明所開發技術於「相關產業之擴散性」。
2. 專利、技轉、產學合作、技術公開推廣等價值創作成效。
3. 計畫成果具體成效及其後續成果承接者。如：主持人及團隊與產業合作或提供政府機關、產業專業諮詢服務實績。計畫以產學合作運作成果作為其績效指標，包含技術供給方（solution supplier）及技術應用方（user）之角色；並請於計畫書中說明合作之法人機構或業界擬參與方式及投入資源（包括研究配合經費、研究人力、獎學金、軟硬體設備等-請參閱附件）

二、 專案優先補助原則

(一)本專案補助具產業效益之多年期整合型前瞻研究計畫；資安特色聯盟計畫則以有研究中心運作機制者優先補助，並請於申請書中載明研究中心名稱、組織架構及運作機制、研究方向、參與團隊、學校資源投入情形。計畫核定將採預核方式通過多年期計畫，惟每年皆須通過成果審查，未達績效指標或不符合專案規劃目標者，必要時將中止下年度計畫之補助。

(二)本專案重視研發成果之價值創造潛力，申請人應提出具有明確之研發企業或法人機構合作合作意願書，應用政府現有雲端軟硬體設備或導入國內業界軟硬體資源，及且有具體企業需求、成果應用規劃、服務模式及執行規劃之計畫（合作研發

可以為學產或學產研合作模式）

(三)本專案鼓勵具國際合作研究關係之計畫（請於申請書中載明合作對象、合作研究內容、合作模式、智財分享模式、合作對象資源投入情形、成果導入應用規劃等，並提出國外合作研究機構明確表達合作意願之佐證）。

三、 推動辦法

(一)推動時程

1. 計畫開始執行日：**106 年 5 月 1 日**。

(二)申請資格

符合科技部專案研究計畫作業要點之申請機構及計畫主持人資格者。

(三)計畫類型

1. 本計畫研究型別以單一整合型計畫(由總計畫主持人將所有子計畫彙整成一本計畫書，且至少需 4 件子計畫參與)為限。
2. 單一整合型每案申請總經費每年不超過 800 萬元為原則。**特色資安聯盟及深耕研究(特色中心)**每案申請總經費每年不超過 1000 萬元為原則。

(四)計畫提案規定

1. 本專案需有產業應用情境。
2. 若所提計畫有與外部機構合作者，除了計畫書內容具體說明研究標的與產業需求的關聯外，請將合作單位之合作確認書(附件)，附加於計畫申請書內，供審查委員參酌。

(五)計畫書格式

1. 計畫書：同科技部專題研究計畫申請書格式。
2. 應填寫附件，並附於計畫書表 CM03 研究計畫內容：請填具附件 2A：參與相關活動承諾書及附件 2B：申請計畫契合優先補助原則檢核表。所提計畫有與外部機構合作者，應填寫外部機構合作確認書（附件 3A）。無具體合作對象或由大學本身主導成果運用者請填寫成果運用規劃表（附件 3B）。並請附上過去執行計畫成效調查（附件 4）供參考。
3. 計畫申請書撰寫時，計畫類別請勾選「一般型研究計畫」；研究型別請勾選「整合型計畫」；計畫歸屬請勾選「工程司」；學門代碼請勾選「E98-專案計畫」:「E9849 **資安前瞻創新研發專案計畫**」，以利作業。
4. 本計畫核定通過後，將列為**主持人執行本部一般專題研究計畫之計畫件數**，惟不列共同主持人之執行件數。

(六)審查流程

1. 初審：依計畫主題，邀請相關學者專家進行書面審查。
2. 複審：依據初審意見及本案宗旨合議決定通過之名單，並得指定一名推動委員負責就個案審查意見與主持人溝通，調整研究計畫之研發內涵。
3. 核定：依本部作業程序核定之。

(七)執行方式

1. 本專案所通過的研究計畫，必須依本司訂定的工作項目來執行計畫，且應落實申請書所提計畫品質管理規範及提供相關文件電子檔給推動委員進行審查，若未依本司所擬定之流程執行並參與各項活動或執行不力者，本部得終止補助。
2. 提報相關文件：
   a. 系統開發階段：需保存測試規劃報告及相關研發記錄。
   b. 成果驗收階段：繳交系統測試報告電子檔，並於成果發表會展示成果。
   c. 結案階段：繳交成果報告書至科技部（依科技部格式）。

詳細作業流程將另行通知，並擇期舉辦說明會向研究計畫之主持人說明。

(八)成果評估：

1. 計畫主持人需自訂技術里程圖、查核點、評量指標，以為評審委員查核之依據。
2. 研究計畫執行期間之各作業階段的成果將由推動委員負責評估並報告。主持人除繳交相關文件外，亦應依科技部規定繳交成果報告。
3. 研究計畫結案時將由本司組成審查委員以現場展示方式評估各計畫執行成果，並向科技部報告。(計畫成果報告主要審查項目包括：需求規格完備度、成果可應用性、技術方案優越性、測試完整性、各期報告完整性）。
4. 本專案各研究計畫之執行成效，將做為下一年度核定補助計畫經費之參考依據。

(九)智財權及技術轉移規定：

本案各研究計畫所產出之原始碼軟體，依據科技部對開放軟體智財權之規定實施之。技術轉移亦依科技部相關規定作業。

(十)相關活動及成果推廣：

為利於各研究計畫之執行及成果推廣，計畫主持人及參與研究人員需在計畫期間參與下述活動：

1. 計畫主持人座談會。
2. 「計畫成果發表會」，計畫主持人得向本部組成審查委員說明及展示計畫成果，並由審查小組進行評選遴選績優計畫團隊。同時也將邀請具有專業知能的產官學研各界人士進行經驗交流，以提昇技術研發能量。績優計畫團隊並由本會推薦參加相關展覽。

四、 其他注意事項

(一)主持人以申請一件本專案研究計畫為限。

(二)本計畫屬專案計畫，恕無申覆機制，且有退場機制。

(三)本計畫之簽約、撥款、延期與變更、經費核銷及報告繳交等，應依本部補助專題研究計畫作業要點、專題研究計畫經費處理原則、專題研究計畫補助合約書與執行同意書及其他有關規定辦理。

(四)其餘未盡事宜，依本部補助專題研究計畫作業要點及其他相關規定辦理。

五、計畫聯絡人

科技部工程司助理研究員 梁雁惠
e-mail： yhliang@most.gov.tw
電　話：（02）2737-7437
科技部工程司副研究員 張哲浩
e-mail： thchang@most.gov.tw
電　話：（02）2737-7525
傳　真：（02）2737-7673
地　址：106 台北市和平東路二段 106 號 16 樓

科技部工程司專任助理 許馨予
e-mail： xyshu@most.gov.tw
電　話：（02）2737-7525
傳　真：（02）2737-7673

附件 1 資訊安全前瞻創新研發計畫重點推動研發主題：
資安前瞻創新研發

項目	主題
主軸一：新興產業與國家基礎建設安全	
物聯網架構與應用（IoT）、工業控制系統（SCADA）安全	● Embedded/IoT/ICS (工業控制系統) 逆向工程研究 ● 研究保護 update/patch Embedded/IoT/ICS 系統 ● Embedded/IoT/ICS (工業控制系統) 入侵偵測系統研究 ● 物聯網實體設備安全研究 ● 物聯網網路架構安全技術研究
5G 基礎建設（SDN/NFV、雲端）安全	● 主機虛擬化安全相關研究 ● 網路虛擬化安全相關研究 ● 虛擬網路內部感染相關研究
金融科技（FinTech）安全	● 金融設備(例如：提款機)安全分析研究 ● 金融網路入侵偵測系統研究 ● 金融網路交易異常監控系統 ● 區塊鏈(Blockchain) 相關安全研究 ● 高準確度身份識別技術研究
主軸二：自動化攻擊防禦技術與攻防演練平台建置	
高等網路入侵偵測與防禦系統（IDS/IPS）及誘捕系統（Honeypot）	● 10G 以上超高吞吐量效能研究 ● HTTP 2.0 DPI 技術研究 ● 以網路封包為基礎(proxyless)的惡意程式偵測與攔截 ● 以網路封包為基礎的網路設備識別 ● 以網路封包為基礎的網路應用程式流量識別 ● 以網路封包為基礎的使用者識別與行為喜好分析
自動化數位鑑識（Forensic）	● 系統還原與資料舉證研究 ● 網路流量鑑識研究 ● 記憶體鑑識研究 ● 磁碟與檔案系統鑑識研究 ● 入侵事件分析自動化
資安大數據研究資料庫	● 惡意程式樣本大數據資料庫 ● 惡意程式檔案自動化分類與溯源研究 ● 惡意程式網路行為自動化分類與識別研究 ● 以 CVE (Common Vulnerabilities and Exposures) 為基礎的大數據泛用型弱點資料庫 ● 以 CWE (Common Weakness Enumeration) 為基礎的程式設計弱點資料庫
	● 雲端攻擊技術(Cyber Attacks in Cloud Computing) ● 執行檔程式弱點自動分析研究

自動化弱點分析與惡意程式特徵碼生成技術	● 弱點攻擊程式(exploit/shellcode)自動生成研究 ● 網路入侵偵測特徵碼(IDS rule)自動生成研究 (含 firewall rule) ● 病毒碼自動生成研究(排除 checksum-based 方法，例如：md5/sha1 等)
基於深度學習之自動化攻擊防禦技術	● 惡意行為風險評估技術研發與平台建置 ● 程式與網路應用服務弱點自動分析技術研發 ● 攻擊與防禦自動化技術研發(含 AI/Data Mining/Machine Learning 等研究)

特色資安聯盟及深耕研究(特色中心)

主題	研究項例
特色資安研究中心	● 行動裝置與 IoT 終端設備之安全研究 ● 前瞻產業網路之機密保護、洩密偵防以及安全檢測研究 ● 關鍵基礎設施的資安與隱私防護研究 ● 資料安全技術與資安管理研究

雲端攻防演練平台及惡意程式資料庫研製

主題	研究項例
深度學習平台研發	● 行動裝置與 IoT 終端設備之安全研究中心 ● 道德駭客技能訓練平台(Wargame) 人才培訓 ● 攻防搶旗賽(Capture the flag, CTF) 攻防競賽 ● 網路挑戰賽(Cyber Grand Challenge, CGC) 實驗平台技術研發 ● 惡意行為風險評估技術研發與平台建置 ● 程式與網路應用服務弱點自動分析技術研發 ● 攻擊與防禦自動化技術研發(含 AI/Data Mining/Machine Learning 等研究)
前瞻資安實驗場域	● 網路安全場域研究 ● 系統安全場域研究 ● 物聯網安全場域研究 ● 行動應用與通訊安全場域研究 ● 智慧家庭安全應用場域研究 ● 智慧城市安全應用場域研究 ● 金融科技安全應用場域研究
惡意程式知識庫創新研發	● 巨量資料快速處理架構 ● 自動化時光沙箱檢測技術研發 ● 行動裝置惡意程式檢測技術研發 ● 網域與網域檢測技術研發 ● 惡意程式知識庫加值應用 ● 惡意程式行為偵測與分類技術研發

新世代誘捕系統與反駭客偵測技術研發	● 誘捕系統部署與架構技術 ● 分散式日誌分析技術 ● 主被動式誘捕系統研發 ● 反駭客偵測系統研究 ● 網路行為自動化分析研究
開放資料創新與營運關鍵技術	● 多態樣檢測資料集研究 ● 視覺化技術 ● 去識別化系統 ● 5G 資通訊安全技術研析 ● 圖像檢索與識別技術

附件2A

承諾書

本人承諾針對所主持**科技部「資安前瞻創新研發」**之研究計畫，願意依照承諾書規定之作業流程執行計畫（包含參與活動、繳交報告書等），詳細內容如下：

預 定 日 期	進行事項	附 註
2017/11~12	期中進度審查	1.各計畫開放專案管理平台，供委員上網檢視審查 2. 整合型計畫/計畫執行不佳者，須出席審查會議，進行期中報告
2018/4	繳交系統測試報告電子檔	依本部規定之規範撰寫，上傳至專案管理平台
計畫執行期間	參加計畫品管會議、專案平台說明會、成果發表會、推廣會議、交流會議、技術公開展示會議等	計畫派員參加
2018/5~8	期末審查暨計畫成果發表會	依本部規定之規範進行期末審查並參與計畫成果發表會
2018/6~8	上傳計畫成果報告書至科技部	依科技部格式

立同意書人 簽名＿＿＿＿＿＿＿＿＿＿

中華民國＿＿＿＿年＿＿＿＿月＿＿＿＿日

附件 2B 申請計畫契合「資安前瞻創新研發計畫」專案優先補助原則檢核表

序號	查核項目	是 ■ ／否□	說明（填■者須作答）
1	是否符合資訊安全實務專案重點研究主題?	□	重點推動研究主題項目：
2	是否有國內合作企業?	□	國內企業名稱：
3	是否與國內企業及法人機構形成研發聯盟?	□	國內企業名稱： 國內法人名稱：
4	是否有國外合作對象?	□	國外機構名稱：
5	是否與國外機構、企業或法人機構形成研發聯盟?	□	國外機構名稱： 國外企業名稱： 國外法人名稱：
6	是否運用國內學界或政府單位現有雲端設備環境？	□	設備提供單位：
7	是否具有**特色資安聯盟及深耕研究**中心運作機制?	□	研究中心名稱： 學校資源投入情形： 參與學者數量： 中心主持人：
8	是否有具體成果運用及價值創造構想?	□	成果運用及價值創造方式： 參與機構或企業： 預定期程：

附件3A 外部機構合作確認書

企業／機構名稱及地址	
成立時間	
員工人數及研發人員數	
主要產品或業務	
公司資本額	
雙方合作方式及擬投入之資源	
雙方合作內容及預期產出之規格	
成果運用及價值創造方式	
成果運用預定期程	
過去成果應用效益（雙方曾有合作案例者請填寫）	
企業／機構及負責人用印	

附件 3B 成果運用規劃表

預定導入機構	
成果運用內容	
成果運用對象	
成果運用期程	
價值創造模式及途徑	
導入機構投入資源規劃	
成果運用機構用印	

附件 4

過去執行成效

一、過去執行過資訊安全或資通領域等計畫，請提供以下各項資料：

項　目	內　容
成果技轉	技移單位： 合作主題： 提供金額： 計畫年度： 計畫名稱：
產學合作	委託單位： 合作主題： 提供金額： 計畫年度： 計畫名稱：
論文發表	論文題目： 投稿單位： 計畫年度： 計畫名稱：
軟體元件	元件名稱： 下載次數： 應用情形： 計畫年度： 計畫名稱：
技術服務	服務對象： 衍生效益： 服務內容： 服務年度： 計畫關聯性：

競賽得獎	競賽名稱： 作品名稱： 獲獎日期： 計畫年度： 計畫名稱：
技術公開推廣	活動名稱： 技術名稱： 活動日期： 計畫年度： 計畫名稱：
專利申請	專利名稱： 發明人： 申請／核准日期： 申請／核准案號： 計畫年度： 計畫名稱：

簽 名＿＿＿＿＿＿＿＿＿＿

中華民國＿＿年＿＿月＿＿日