經濟部 111 年度

《臺灣資安卓越深耕-半導體及資通訊供應鏈資安關鍵技術發展計畫》

合作研究計畫

《供應商管理工具及晶片溯源管控機制及工具規劃》

建議書徵求文件

財團法人資訊工業策進會

中華民國 111 年 3 月

111 年度合作研究計畫建議書徵求文件

一. 簡介

近年來陸續發生多起晶片漏洞與攻擊事件，如 CPU 的 Meltdown、Spectre、Foreshadow 等漏洞；FPGA 的 Starbleed 漏洞；DRAM 的 Rowhammer 攻擊等，影響使用 Qualcomm、Intel、AMD、IBM、ARM 等晶片之電腦、平板及手機設備。觀察目前發現的漏洞，幾乎都是因晶片設計缺陷而造成，由於晶片的設計與產製特性，要在發布後像軟體一樣以更新方式進行安全性修補幾乎不可能，因此更需要建立安全的供應商管理系統，以避免最終產品發生與資安相關的問題。

由於國內 IC 設計公司多數尚未具備符合國際公認之軟體安全開發機制，造成打入國際供應鏈受阻，爰此，臺灣資安卓越深耕-半導體及資通訊供應鏈資安關鍵技術發展計畫 (以下簡稱主計畫)將延續 FY110 科專計畫之研發成果，完善安全軟體開發管理框架，持續發展安全軟體開發合規輔助工具，並將觸角延伸至供應商，除使 IC 設計公司可掌握矽智財(IP)供應商之安全軟體開發生命週期合規狀態，並整合下游晶片模組廠商及系統整合廠商，規劃建立國內晶片供應鏈資安生態體系。面對國際買家之相關稽核亦可提出包含供應商之佐證資料。

本合作研究計畫因應主計畫之目標，發展晶片供應商安全料件清單模組，重點研發晶片供應商管理工具，提升晶片供應鏈安全，使我國晶片供應鏈產品品質保持世界級競爭優勢。

二. 計畫目標

本合作研究計畫目標為建置符合晶片供應鏈需求的供應商管理工具，導入晶片供應鏈廠商進行場域實證，及調查晶片產業供應鏈現況，並蒐集相關資安需求，作為主計畫建立晶片軟體安全開發框架之參考。

三. 計畫範圍

本計畫預期工作項目包括：

1. 晶片設計流程及供應商管理組態項目研究

藉由晶片設計業者及晶片產業下游供應鏈業者諮詢，研討晶片內部設計流程及下游供應商管理應具備組態項目，並產出晶片供應鏈資安管理需求分析等報告。

2.晶片供應商管理平台開發

開發整合晶片供應商管理平台，與晶片設計流程及下游供應鏈業者建立關聯並開發使用者介面，供應商管理平台內容內容包括：晶片設計廠商及晶片下游供應鏈業者之安全料件清單上傳、供應鏈安全料件清單管控及介接主計畫之安全活動支援工具進行介接等。

3. 晶片供應商管理平台的場域實證

藉由晶片產業諮詢，尋找與晶片供應商管理平台合作意願之晶片設計廠商或下游供應鏈廠商，並導入 3 家廠商進行場域實證。

4. 晶片溯源規格分析研究

藉由研析國際現行各種溯源機制運作與配套管理流程，包含國際半導體產業協會(SEMI)供應鏈可追溯性標準，避免供應鏈攻擊，如仿冒、回收、重新標記、複製等威脅。透過研析，從中援引、取用可行之機制與流程歸整為溯源規格開發建議，提供晶片設計供應鏈溯源規格之開發功能與規格需求參考。

四. 預期成果

1. 完成 5 家廠商訪談，並產出晶片供應鏈資安風險評估分析內容、晶片產業供應鏈管理需求分析內容、晶片供應商管理平台一式與測試報告一份、晶片溯源規格分析研究報告一份。
2. 完成 3 家晶片供應鏈廠商場域實證，並產出 1 份晶片供應鏈場域導入成果報告，描述場域實證成果。

※前述成果如有專利構想或專利申請產出時，需注意專利申請之新穎性(novelty)。因凡經公開發表之研發成果，如擬申請專利，須於公開發表後 6 個月內完成，前述成果如是以論文方式公開發表，將無法取得大陸與歐盟等國之專利。

五. 執行方式

本計畫運用業界的研發能量與領域智識，配合主計畫「臺灣資安卓越深耕-半導體及資通訊供應鏈資安關鍵技術發展計畫」提供晶片安全軟體開發管理平台各資安工具模組，進行如「計畫範圍」所定義分析與開發。

預計將結合業界之研發能量與領域實務面經驗，回饋給主計畫技術研發方向，透過雙方相互合作討論的方式來進行。本計畫亦需提供相關系統之教育訓練及經驗分享機制，藉此增進本會研究人員的專業能力，以提升本合作案成果之效益，相關執行方式步驟如下：

1. 辦理 5 家廠商訪談。
2. 完成晶片供應商安全料件管理系統開發。
3. 導入 3 家晶片供應鏈廠商進行場域實證。

六. 計畫期程及預估計畫總經費

計畫執行區間： 111 年 5 月 1 日 至 111 年 12 月 15 日

總經費：1,000,000 元（含稅）

七. 驗收標準

項次	交付項目	交付內容	數量	交付型態	交付期限
1	晶片設計流程及供應商管理組態項目研究報告	研究報告內容應包含： ● 晶片供應鏈資安風險評估分析 ● 晶片產業供應鏈管理需求分析 ● 晶片設計流程之IP library管理組態及資料上傳標準分析 ● 晶片下游供應商管理組態項目及資料上傳標準分析。	1式	電子檔	111年 6月15日
2	晶片溯源規格分析研究報告	報告內容應包含： ● 國際現行溯源機制運作與配套管理流程（如國際半導體產業協會(SEMI)供應鏈可追溯性標準 ● 國際常見供應鏈攻擊方式，如仿冒、回收、重新標記、複製等威脅。 ● 溯源機制、流程與溯源規格開發建議。	1式	電子檔	111年 8月15日
3	晶片供應商管理平台	平台內容應包含下列功能： ● 晶片設計廠商晶片安全料件清單上傳 ● 晶片下游供應鏈廠商安全料件清單上傳 ● 供應鏈安全料件清單管控 ● 安全軟體開發管理框架之安全活動支援工具介接	1式	電子檔 (程式、原始碼)	111年 11月15日
4	晶片供應商管理平台測試及安全掃瞄報告	應針對下列功能進行測試： ● 晶片設計廠商晶片安全料件清單上傳 ● 晶片下游供應鏈廠商安全料件清單上傳	1式	電子檔	111年 11月15日

項次	交付項目	交付內容	數量	交付型態	交付期限
		● 供應鏈安全料件清單管控 ● 安全軟體開發管理框架之安全活動支援工具介接			
5	晶片供應商管理平台使用手冊	晶片供應商管理平台各項功能使用手冊說明	1 式	電子檔	111 年 11 月 15 日
6	晶片供應鏈場域導入成果報告	藉由晶片產業諮詢，尋找與晶片供應商管理平台合作意願之晶片設計廠商或下游供應鏈廠商，導入 3 家廠商進行場域實證	1 式	電子檔	111 年 11 月 30 日

1. 本專案製作完畢後，乙方需將系統移轉至正式機器上，並可執行運作；並能於指定環境建立 Demo Site。
2. 乙方須提供程式、資料庫原始碼，提供甲方留存。
3. 為建立團隊對於相關程式運作機制及操作之了解，提供教育訓練。
4. 進度討論會議：每二週至少召開一次進度研討會議。

八. 技術能力需求

本合作研究計畫執行人員須具備資訊領域相關基礎知識背景包含：

1. 具備系統規劃整合與建置維運經驗。
2. 具晶片供應鏈廠商業務合作經驗。
3. 其他：如熟悉 OWASP Top Ten 攻擊手法、安全料件資料格式或 CVE Details 分析及運用 等。