115年資訊（安）主管資安研習交流會議紀錄

一、會議時間：115年7月16日下午2時

二、會議地點：集思臺大會議中心國際會議廳

三、議題報告：(略)

四、座談與意見交流會議主持人：資通安全署周副署長智禾

五、參加人員：參訓機關資訊(安)主管（略）

六、會議結論

(一)危害國家資通安全產品之認定及提報機制

1. 各機關可依「危害國家資通安全產品審查辦法」規定，針對有疑慮之資通訊產品，由該辦法第2條所訂之機關填具提報表並檢附相關文件[含物料清單（BOM）及軟體物料清單（SBOM）]送交資通安全管理法主管機關審查。
2. 目前依行政院秘書長109年12月18日院臺護長字第1090201804A 號函，全面禁止公務機關使用及採購大陸廠牌資通訊產品，其核心範圍涵蓋軟體、硬體與資訊服務，並採取從嚴認定標準。
3. 考量目前係由採購機關先行針對使用及採購標的是否涉危害國家資通安全產品，後續資安署將研議由廠商主動揭露並切結相關資訊之可行性，以減低機關負擔。

4. 針對資通訊產品之產地及零組件限制，依現行採購法規定，各機關可依採購案件之性質、使用情境及資安風險，於招標文件或契約中訂定。

(二)政府機關使用人工智慧工具之資安管理

. 各機關使用人工智慧工具，應依行政院相關指引辦理，不得將國家機密、機敏資料或其他不得公開之資訊上傳至外部人工智慧平臺。使用免費或公開版本之人工智慧工具時，應避免輸入機關內部資料、個人資料及其他敏感資訊。

. 如使用具企業授權或資料保護機制之人工智慧服務，仍應依資料敏感程度及機關內部規定審慎評估，不得因業者聲稱零資料保留及不進行模型訓練，即逕行上傳機密或機敏資料。各機關得視實際需求，導入人工智慧使用管理、瀏覽器活動監控或資料外洩防護等工具，以掌握同仁使用情形及降低資料外洩風險。

(三)資安專業訓練及證照課程量能

. 建議各機關彙整內部訓練需求，並由上級機關統籌所屬機關需求後，洽訓練機構研議開設專班。專班之開課人數及相關條件，由各訓練機構依實際情形訂定。

. 機關確有課程或訓練名額需求，得向資安署反映，作為後

續課程規劃之參考。

(四)資安專職人員之認定及人力配置

資安專職人員係指以資通安全業務為核心業務之人員，得兼辦其他業務，惟其工作安排仍應以資通安全業務為優先，並確保資安工作之推動及執行量能。

(五)共同供應契約產品之資安強化措施

. 資安署已與數產署合作推動委外服務廠商之聯合查核，部分受查對象亦為共同供應契約廠商。另漏洞獎勵機制前期以資通訊設備為主，後續將研議納入共同供應契約相關系統或產品。

. 共同供應契約產品提供 SBOM 目前以鼓勵方式推動，尚未全面強制。另考量部分代理商無法取得原廠 SBOM，或廠商將 SBOM 視為內部營業資訊，相關制度將配合產業實務逐步推動。

. CBOM 及 AIBOM 等新興供應鏈資訊管理機制，將納入後續政策研議。

(六)後量子密碼遷移規劃

.政府將持續參考金融業後量子密碼推動及實作經驗，規劃

政府機關整體遷移政策。預計於115年度第四季公布後量子密碼遷移策略文件及實務參考手冊，說明政府整體推動方向及規劃藍圖。

. 未來將研議透過政府採購、共同供應契約及需求端規範，逐步引導資通訊產品具備 PQC Ready 能力。

(七)政府憑證及電子簽章國際信任機制

有關自然人憑證納入至 AATL 等議題，因涉及跨機關業務協調，尚須進一步評估整合及推動之可行性，資安署將再行研議。

七、散會：下午5時10分。