國家資通安全會報第1次委員會議紀錄

壹、時間：115年7月9日（星期四）下午3時

貳、地點：行政院第1會議室

參、主席：鄭召集人麗君　　紀錄：林煒智

肆、出列席人員：如附簽到表

伍、主席致詞：（略）

陸、報告事項：

一、 數位發展部（下稱數發部）提報「國家資通安全會報運作規劃」一案，報請公鑒。

決定：

(一)洽悉。

(二)為落實本會報新制架構，請數發部充分發揮幕僚工作會議功能，加強跨部會先期協調；另新制特設成立專案小組之雙軌機制，請各部會積極運用，依轄管業務需求及新興資安風險趨勢，評估成立特定議題專案小組，並將評估結果提送數發部彙辦，以發揮國家整體資安防護之統籌協調綜效。

(三)本會報原則每半年召開一次，必要時召開臨時會議。若有緊急成立特定專案小組之需求，必要時可先行由幕僚機關簽陳會報召集人核准，後續提報本會報備查。

(四)本會報各項決議及交付事項，請各部會務必貫徹執行。後續由數發部定期追蹤管考，並將辦理情形納入機關績效評核；期勉各部會密切配合，全力推動「國家資通安全發展方案（第七期）」等重大資安政策，確保各項施政穩健落實。

二、 數發部提報「國家資通安全發展方案 114 年成果報告」一案，報請公鑒。

決定：

(一)洽悉。

(二)感謝各部會在資通安全防護上的努力，114 年在全社會資安防禦、提升關鍵基礎設施（CI）防護韌性、擴大本土資安產業規模與國際輸出，以及拓展 AI 新興科技應用與國際合作等四大策略上，皆已展現初步且具體的亮點成果，值得肯定。

(三)有關「壯大我國資安產業」策略之 APP 驗證機制，請各目的事業主管機關評估及管理所轄產業相關 APP 之資安風險。另與國際標準接軌至為重要，我國無人機驗證機制已與 Green UAS 接軌，並正爭取 Blue UAS 驗證執行資格，未來無人載具（如自駕車、無人機等）均需進行高標準資安檢測，請經濟部、數發部等相關部會提早落實國際標準接軌工作。

(四)現行產業監理制度多偏重上市前檢測與登錄，為避免受檢之黃金樣本無法確保其市售後之品質，請經濟部、數發部就無人載具（如自駕車、無人機等）部分，考量依風險分級（低、中、高）建立「前、後市場稽查」雙軌制度，相關實驗室建置與資源配置雖需時間籌備，仍請相關部會先行啟動規劃並共同推動。

(五)為提升關鍵基礎設施資安防護，數發部已成立國家 CI 資安防護團隊執行威脅狩獵與設施檢測，請各 CI 主管

機關務必督導所轄提供者，全力配合各項檢測作業與後續弱點改善，持續強化關鍵基礎設施面對網路威脅的整體韌性。

三、 數發部提報「115 年資通安全業務推動及重點工作」一案，報請公鑒。

決定：

(一)洽悉

(二)115 年資通安全稽核計畫准予備查，請各受稽機關配合整備相關資料；另請各機關持續配合推動「受託者資安聯合稽核」計畫，並妥善規劃擴大邀請四院及地方政府參與聯合稽核事宜，以降低重複稽核負擔。

(三)為防範相同資安風險在機關重複發生，請各機關首長、資安長及資安主管負起系統性檢視責任，遵循「最小權限原則」並落實定期帳號權限盤點、電子郵件社交工程演練及委外廠商監督管理等資通安全管理機制。另請數發部強化與各機關資安主管之定期、不定期聯繫，及時分享資安風險情資，各主管亦務必於機關內貫徹宣導，杜絕風險樣態反覆發生。

(四)請各機關務必落實推動「危害國家資通安全產品審查辦法」，針對品牌、產地、第三地及軟硬體零組件等均應全面納入管理；除政府機關外，各 CI 主管機關亦應督導所轄提供者強化日常安全管理機制。

(五)數發部已於 115 年 7 月 1 日公布「公務出國資通訊設備管理須知」，請各機關同仁公務出國時，務必依管理須知落實設備防護，嚴防公務機密外洩，並請數發部透過資

安稽核評核各機關落實情形。

(六)針對「廣告電子看板安全管理須知」,請依規劃及各方意見完備相關內容，並辦理報院頒布事宜，未來各機關應配合強化看板安全管理，以防範錯假訊息與認知作戰。

(七)關鍵基礎設施攸關國家運作與民生安全，本屆跨國網路攻防演練（CODE 2027）聚焦「交通主題」並以「藍隊」防禦為主體，請交通部充分發揮主管機關協調功能，督導所管之特定非公務機關積極參演，以實戰強化關鍵基礎設施資安同仁的防護能量。

柒、討論事項：

一、 數發部提報「前沿 AI 模型對國家資通安全之影響與後續因應」一案，提請討論。

決議：

(一)近期國際間高度關注前沿 AI 模型展現出的強大自動化漏洞挖掘與攻擊能力，為避免駭客攻擊速度遠超人工修補速度而造成的國安風險，請數發部邀主要相關部會組成策略小組，研議我國短、中、長期防護因應策略，並關注最新的 AI 技術發展，尋求合作解方，滾動修正短中長期防護因應計畫，以有效應對可能的風險。

(二)待數發部策略小組提出漏洞檢視並發布漏洞管理指引後，請各機關務必依循並儘速落實資訊資產盤點與保護，加速修補漏洞或採行防護措施。另請數發部資安署持續透過強化產品上架共同供應契約機制、強化供應鏈資安防護及中長期國際合作，以提升我國面對 AI 威脅之防禦能量與整體資安韌性。

(三)行政院長已於115年6月主持之國家人工智慧戰略特別委員會中裁示，政府應盤點AI所需之硬體、軟體及應用服務，積極建構新基礎建設，包含算力、能源、網路資訊安全、資料安全、AI運用與服務安全、AI評測機制及法規調適等。因應前沿AI模型對資安之影響，請數發部與相關部會提出我國攻守兼備之整體因應對策，必要時提出新計畫或結合既有計畫推動，並請主計總處優先支持匡列相關預算。

二、 外交部提報「成立外館網際防護專案小組」一案，提請討論。

決議：

(一)鑒於外交業務屬性機敏，向為駭客攻擊目標，尤以外館所在駐地資訊環境非由我掌控，且派遣駐外人員之國內機關甚多，實有成立「外館網際防護組」統合協調之必要。請外交部主責辦理，並會同相關派駐機關儘速完備運作機制，以建構我國海外駐地之資通安全防禦網絡。

(二)本案照案通過，同意外交部成立「外館網際防護組」，後續請外交部透過定期會議，統合協調各駐外機關之資安作業，持續加強各項防護作為，請各機關積極配合，以提升外館整體防護量能。

捌、臨時動議：無

玖、散會(下午4時40分)