◎資通安全維護宣導

—〈資安法〉上路！ 建構資通安全新時代—

《資通安全管理法》(下簡稱:〈資安法〉)於 108 年 1 月 1 日上路，《公務機關所屬人員資通安全事項獎懲辦法》也同步實施。依據該等辦法，全國公務機關必須訂定資通安全維護計畫、資安事件通報及應變機制，違反者，資安人員最重將遭到記一大過的處分。

前言

當大家透過手機或電腦享受網路便利的同時，駭客也無時無刻伺機入侵，輕者個人資料外洩，重者公司商業機密遭竊，甚至有政府機關因而停擺，可見資訊安全已是刻不容緩之議題。由於缺乏一套以風險管理為基礎，規範整體資通安全的專法，行政院參酌先進國家立法原則，並考量我國社經環境與法規制度，研訂〈資安法〉草案，於 107 年 6 月 6 日總統華總一義字第 10700060021 號令制定公布，行政院另於同年 11 月 21 日訂定發布《資通安全管理法施行細則》、《資通安全責任等級分級辦法》、《資通 安全事件通報及應變辦法》、《特定非公務機關資通安全維護計畫實施情形稽核辦法》、《資通安全情資分享辦法》及《公 務機關所屬人員資通安全事項獎懲辦法》等 6 種配套規定，且已自 108 年 1 月 1 日 施行。有鑑於各界面對上路不久的資安新法，一時恐難探究竟，故本文歸納分析之，期能提供各界參考遵行。

〈資安法〉相關重點

一、立法目的為因應網際網路及其他資通科技快速發展與普及，〈資安法〉的立意即是加速建構完善的國家資通安全環境，以保障國家安全，維護社會公共利益，並建立以風 險管理為核心的機制，要求規範對象於發生資安事件時，能立即通報並應處。另一目的則盼此帶動我國資安科技研發、資安服務、資安教育等產業發展。在此說明，法條中所稱「資通安全」，係指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。而所謂「資通安全事件」，則指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政 策之威脅。

二、規範對象 〈資安法〉規範對象分為兩大類，其 一是公務機關，係指依法行使公權力之中央、地方機關（構）或公法人，但不包括軍事機關及情報機關；另一對象則是特定非公務機關，此限於關鍵基礎設施提供者、公營事業及政府捐助之財團法人，並不及於一般民眾。前述所稱關鍵基礎設施，指實體或虛擬資產、系統或網路，其功能一旦停止運作或效能降低，對國家安全、社會公共利益、國民生活或經濟活動有重大影響之虞者，例

資安法規範對象包含公務機關與特定非公務機關，後者包含關鍵設施提供者、公營事業及政府捐助之財團法人，不及於一般民眾。（圖片來源：行政院國家資通安全會報技術服務中心，https://www.nccst.nat.gov.tw/HandoutDetail?lang=zh&seq=1280）

如電力、交通、金融、醫 療、水資源、通訊傳播、緊急救援等系統 或網路。

提醒注意者，依據〈資安法〉第 9 條規定，公務機關或特定非公務機關，於本法適用範圍內，委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。

三、應行義務〈資安法〉乃就公務機關、特定非公務機關兩種規範對象分別訂定其相關義務。在公務機關資通安全管理部分，於本 法第 10 至 15 條設有明文，重點有公務機關應符合其所屬資通安全責任等級之要求，並考量所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件， 訂定、修正及實施資通安全維護計畫，而 《資通安全管理法施行細則》第 6 條則明確列舉資通安全維護計畫應包括之 13 點必要事項；由機關首長指派副首長或適當人員兼任資通安全長，負責推動及監督機關內資通安全相關事務設置；每年向上級或監督機關提出資通安全維護計畫實施情形；稽核其所屬或監督機關之資通安全維護計畫實施情形，受稽機關有缺失或待改善者，應將改善報告送交稽核機關及上級或監督機關，有關改善報告之內容,在《資通安全管理法施行細則》第 3 條明列 4 項必要事項；為因應資通安全事件，應訂定通報及應變機制，當知悉資通安全事件時，除應通報上級或監督機關外，並應通報主管機關，另應向上級或監督機關提出資通安全事件調查、處理及改善報告，並送交主管機關；所屬人員對於機關之資通安全維護績效優良者，應予獎勵。另在特定非公務機關資通安全管理部分，於本法第 16 至 18 條予以規範，重點首先是中央目的事業主管機關應於徵詢相關公務機關、民間團體、專家學者之意見後，指定關鍵基礎設施提供者，報請主管機關核定，並以書面通知；關鍵基礎設施提供者應符合其所屬資通安全責任等級之要求，訂定、修正及實施資通安全維護計畫,並向中央目的事業主管機關提出資通安全維護計畫實施情形，有缺失或待改善者亦應提出改善報告，而中央目的事業主管機關應辦理稽核；關鍵基礎設施提供者以外之特定非公務機關，比照前述規範訂定、修正及實施資通安全維護計畫，中央目的事業主管機關得要求其提出資通安全維護計畫實施情形，並得辦理稽核；特定非公務機關為因應資通安全事件，應訂定通報及應變機制，於知悉資通安全事件時，應向中央目的事業主管機關通報，並提出資通安全事件調查、處理及改善報告；如為重大資通安全事件者，並應送交主管機關。

此外，依據《資通安全責任等級分級辦法》，公務機關及特定非公務機關之資 通安全責任等級，係根據業務所涉機敏程度及有無涉及關鍵基礎設施為判斷標準，並將資通安全責任等級由高至低，分為 A、 B、C、D、E 等

5 級，且就不同等級在管理面、技術面、認知與訓練等面向，分別規範其應辦事項。

四、相關罰則〈資安法〉第 19 條規定，公務機關所屬人員未遵守本法規定者，應按其情節輕重，依相關規定予以懲戒或懲處。第 20 條明文，特定非公務機關若未依本法訂定、修正或實施資通安全維護計畫；違反資通安全維護計畫法定必要事項；未向中央目的事業主管機關提出資通安全維護計畫之實施情形；未訂定資通安全事件之通報及應變機制，或違反法定必要事項；未向中央目的事業主管機關或主管機關提出資通安全事件之調查、處理及改善報告；違反有關通報內容之規定，有上述情形之一者，由中央目的事業主管機關令限期改正，屆期未改正者，按次處新臺幣（下同）10 萬元以上 100 萬元以下罰鍰。另為強化通報機制，第 21 條明定，特定非公務機關未通報資通安全事件，由中央目的事業主管機關處 30 萬元以上 500 萬元以下罰鍰，並令限期改正；屆期未改正者，按次處罰之。

結語

由上可知，不論是公務機關或者特定非公務機關，均須界定資通安全責任等級及訂定資通安全維護計畫，方能依法推動資通管理，現雖定有相關法令可供遵循，然而法條內容錯綜複雜，若未瞭解法規、審慎訂定並落實執行，恐失立法美意。申言之，各機關首要之務即是釐清資通安全責任等級及核心業務，因兩者均攸關資通系統之後續安全管理，可說牽一髮而動全 身。透過本文，希望協助公務機關及社會大眾認識這套資安專法，並共同為建構完善的國家資通安全環境攜手努力，以避免自身及國家權益遭駭。

臺中榮民總醫院提醒您也關心您！