「資通安全管理法(草案)」民間團體座談會紀錄

壹、時間：105 年 9 月 8 日(星期四)上午 10 時

貳、地點：臺大醫院國際會議中心 403 會議室

參、主席：簡處長宏偉　　紀錄：賴世榮

肆、出席人員：(如附簽到單)

伍、主席致詞：(略)

陸、報告：資通安全管理法(草案)說明

柒、綜合討論

一、出席人員主要關心議題（依議題順序）:

(一)有關受指定之非公務機關事項

1. 非公務機關被指定而納入本草案適用之條件及界線應力求明確，倘只透過中央目的事業主管機關指定，範圍恐太大，同時亦造成法的不確定性。
2. 美國的資安專法 FISMA 僅規範公務機關，並未涉及民間部分，建議與關鍵基礎設施無關之非公務機關，不適用本草案。
3. 建議電商業者應回歸個資法之規範，並從該法訂定專章配合執行。
4. 承攬政府機關標案之非公務機關，應釐清是否為本草案之指定對象。
5. 日、韓所訂之資安法規係限縮於關鍵基礎設施，並無指定特定行業之規定；而歐盟作法與本草案設計亦不同，本草案部分條文仍具不確定性。

(二)有關行政檢查事項

1. 因個資法已訂有行政檢查之規定，建議不須在本草案再行訂定，避免疊床架屋之疑慮。
2. 因司法警察主要任務在於犯罪偵查，本草案並無刑事相關規定，建議刪除司法警察陪同執行行政檢查相關內容。

(三)有關委外辦理事項

1. 建議委外監督部分應訂定監督標準以利遵循。
2. 本草案第 8 條受託者委外監督部分，建議可限縮在受委託範圍。

(四)有關關鍵基礎設施範疇事項

1. 本草案第 2 條關鍵基礎設施定義，其中通訊傳播部分，建議應釐清是否含括 Line、Facebook 等即時通訊軟體。
2. 本草案第 2 條關鍵基礎設施已含括高科技園區之實體或虛擬資產，倘公司設在高科技園區，其所發放之紅利點數是否即為本草案所稱之實體或虛擬資產，建議應於細則或子法中敘明。

(五)有關行政院及中央目的事業主管機關權責事項

1. 本草案第 17 條第 5 項，有關發生重大資通安全事件時，行政院或中央目的事業主管機關得公告與事件相關之必要內容及因應措施部分，建議應明確說明係由行政院或中央目的事業主管機關進行公告。
2. 瓦斯業屬於關鍵基礎設施，惟其主管機關並非單一，倘涉及管線部分，其主管機關為通傳會，亦有部分業者之主管機關為退輔會，建議能明確劃分。
3. 鑑於電信業已適用許多法規命令，其中亦包括資安義務之要求，建議應釐清本草案與其他法規之適用區別。
4. 本草案第 6 條已規範行政院可進行查核，惟第 16 條亦規範中央目的事業主管機關可進行查核，恐造成業者疲於應付機關查核，建議應統一權責單位。

(六)有關罰則事項

1. 經與個資法比對後，本草案之罰則相對較重，有關資通安全維護計畫之內容、修正等涉及罰則部分，建議應訂定參考標準以利業者遵循。
2. 除訂定罰則外，建議應提供相關獎勵、輔導措施。
3. 本草案第 19 條、第 22 條部分，建議依比例原則，先

令限期改正後再課予罰緩。

(七)有關通報應變機制事項

1. 本草案第 17 條有關資通安全事件通報時機，電商業者在資安事件發生時往往並不知情，等到發現時已是事後，同時本草案沒有通報就立即開罰，對業者負擔過大，建議調修通報時機相關內容。
2. 目前金管會已有相關通報機制，建議從既有管道與機制，由中央目的事業主管機關通報行政院。

(八)其他事項

1. 建議於本草案中保障相關預算、人力，並與各部會建立資安人才培育機制，以及一致之認證標準。
2. 境外單位是否適用本草案，倘本草案只規範本國業者，恐致產業外移，建議應審慎評估。
3. 本草案已訂定矯正預防措施，目前 ISO 27001 已將預防部分移除，建議本草案一併考量。
4. 建議於本草案第 2 條增訂重大資通安全事件之定義。
5. 建議可透過國外資安事件之蒐集整理，由政府建立整體資安防護系統，以抵擋境外惡意攻擊，進而提升我國資通安全。
6. 考量國軍部隊具特殊任務屬性，建議不須於本草案增列當發生大規模資安事件致關鍵基礎設施停止運作時，可發動國軍部隊提供必要協助之規定。

二、請針對出席人員意見，參酌是否調整草案內容。

捌、散會：中午 12 時 10 分