立法院法制局法案評估報告　　編號：1251

本報告僅供委員參考

資通安全管理法草案評估報告

法制局 陳淑敏、曾耀民 撰

中華民國 106 年 7 月

資通安全管理法草案評估報告

目次

摘要 3

壹、背景說明 5

貳、立法要點 8

叁、問題研析與建議 10

一、為使構成要件明確化，建議宜將關鍵基礎設施加以明確定義（草案第 2 條第 1 項第 6 款）.....10

二、為求法律文字表達精簡，建議刪除「依第十五條第一項規定」文字（草案第 2 條第 1 項第 7 款）.....13

三、為求語意明確，建議增列重大資安事件之定義（草案第 2 條第 1 項第 8 款）.....14

四、資通安全政策攸關國家安全，建議每 2 年公布國家資通安全情勢報告及資通安全發展方案，以符現況所需與保持彈性（草案第 4 條）.....14

五、為建立事權統一之管理機制，非公務機關資通安全維護計畫實施情形之稽核宜由中央目的事業主管機關擬訂，報請行政院核定之（草案第 6 條、第 15 條、第 16 條及第 19 條）.....16

六、公務機關尤其應該重視資通安全風險，以提升資通安全能量；建議納入「年度評估報告」，以加強系統化資通安全風險管理（草案第 11 條）.....20

七、草案既有罰則之專章，建議將公務機關所屬人員之懲戒與懲處改列至罰則專章(草案第 14 條第 2 項改列為第 19 條）

.....22
八、重大資通安全事件之公告時間應明確且快速，以避免不確定性及延誤時效（草案第 17 條第 5 項）.....22
九、進入非公務機關場所檢查，其程序應更嚴謹與完備，以符合正當法律程序原則，避免造成侵權之虞（草案第 18 條第 1 項）.....23
十、法案性別與人權影響評估.....33
肆、結論與建議.....33
伍、條文對照表.....35
參考文獻.....73
附錄 76
一：「資通安全管理法草案」評估報告（初稿）座談會紀錄及參採情形.....76
二：行政院法案及性別影響評估檢視表.....89
三：立法院法制局法案性別與人權影響評估檢視表.....108

摘要

近來連續 2 大資訊安全事件，正考驗台灣資安攻防能力。其一為國內偵破史上最大宗 1.7 億筆個資外洩案，政府系統疑遭破解；另一為「WanaCry pt0r 2.0」的勒索病毒正在全世界肆虐，政府單位及企業全面戒備。本草案業經排入第 9 屆第 3 會期第 14 次會議議程報告事項，會議決定：「交司法及法制委員會審查。」本報告針對草案內容進行檢討分析，並就其性別與人權影響評估結果加以檢視及分析，提出修法建議如下，以供委員問政及修法之參考：

一、為使構成要件明確化，建議宜將關鍵基礎設施加以明確定義（草案第 2 條第 1 項第 6 款）

二、為求法律文字表達精簡，建議刪除「依第十五條第一項規定」文字（草案第 2 條第 1 項第 7 款）

三、為求語意明確，建議增列重大資安事件之定義（草案第 2 條第 1 項第 8 款）

四、資通安全政策攸關國家安全，建議每 2 年公布國家資通安全情勢報告及資通安全發展方案，以符現況所需與保持彈性（草案第 4 條）

五、為建立事權統一之管理機制，非公務機關資通安全維護計畫實施情形之稽核宜由中央目的事業主管機關擬訂，報請行政院核定之（草案第 6 條、第 15 條、第 16 條及第 19 條）

六、公務機關尤其應該重視資通安全風險，以提升資通安全能量；建議納入「年度評估報告」，以加強系統化資通安全風險管理（草案第 11 條）

七、草案既有罰則之專章，建議將公務機關所屬人員之懲戒與懲處改列至罰則專章（草案第 14 條第 2 項改列為第 19 條）

八、重大資通安全事件之公告時間應明確且快速，以避免不確定性及延

誤時效（草案第 17 條第 5 項）

九、進入非公務機關場所檢查，其程序應更嚴謹與完備，以符合正當法律程序原則，避免造成侵權之虞（草案第 18 條第 1 項）

資通安全管理法草案評估報告

壹、背景說明

我國目前與資通安全相關之規範，適用於公務機關者，除適用對象較為廣泛之刑法妨害電腦使用罪罪章及個人資料保護法等外，另有行政院及所屬各機關資訊安全管理要點、行政院及所屬各機關資訊安全管理規範、國家資通安全通報應變作業綱要等規定；上述規定中，屬法律者，其規範目的各異，而適用時或僅就實害之結果進行處罰，或其保護客體僅以特定類型之資料為限，並非針對資通安全管理為整體考量而制定；其餘規定對資通安全管理雖定有較細節之規範，但其位階較低，且規定分散，適用上難免不足。至於適用於非公務機關之規定，因其立法目的不同，其適用範圍、保護客體與規範對象亦有差異，無法作為各非公務機關共通遵循之標準，難以帶動其整體資通安全能量。此外，無論是適用於公務機關或非公務機關之規定，均無以資通安全為主要考量，並要求以風險管理為核心，建立完整資通安全維護計畫及通報應變相關機制者，此現況與國際上目前資通安全管理之趨勢尚有落差。國際近年資通安全之政策，許多先進國家係以制定專法之方式對資通安全議題加以規範，例如：美國有聯邦資訊安全現代化法、網路安全法；日本則制定網路安全基本法；在國際組織部分，歐盟亦訂定網路與資訊系統安全指令；透過專法之制定，協助公務機關及關鍵基礎設施提供者等非公務機關，認知其自身資通安全責任、進而理解並因應資通安全風險，增進自身資通安全能力[1]。

[1] 立法院第 9 屆第 3 會期第 13 次會議議案關係文書，院總第 1570 號　政府提案第 15966 號，修正草案總說明。

行政院於 90 年 1 月成立「國家資通安全會報」(以下簡稱資安會報),以統籌並加速我國資通安全基礎建設工作,以 4 年為一週期,陸續推動二期「建立我國通資訊基礎設施安全機制計畫」及二期「國家資通訊安全發展方案」。同年 3 月規劃成立「行政院國家資通安全會報技術服務中心」(以下簡稱技服中心),除協助資安會報逐步建置政府機關分級管理、國家資通安全防護管理平臺(NSOC)等重要機制外,並提供各政府機關事前安全防護、事中預警應變、事後復原鑑識等資通安全技術服務。考量整體資安情勢日趨嚴峻,行政院復於 100 年 3 月 7 日修正「行政院國家資通安全會報設置要點」,成立「行政院資通安全辦公室」(以下簡稱資安辦)。配合 101 年 1 月 1 日行政院院本部組織再造,資安辦成為行政院所設常設性任務編組,「技服中心」於 102 年 1 月 1 日起,改由資安辦委辦及督導[2]。鑒於資通安全業務涉及國家安全,不宜長期以委外方式辦理,且資通安全具高度技術性及專業性,於 100 年行政法人法公布後,相關部門即積極研議及規劃推動技服中心行政法人化,期融合公、私組織之優點與特性,持續強化國家資通安全防禦能量。

另考量科技部具有科技專業,可實質整合產官學研資源,強化資通安全技術研發及服務能量,行政院爰於 103 年 5 月 22 日指定科技部為資通安全之主管機關,並為技服中心行政法人化後之監督機關;「國家資通安全科技中心設置條例」業於 104 年 12 月 14 日三讀通過,同年 12 月 30 日公布,105 年 1 月 20 日施行,技服中心依該條例轉型為行政法人「國家資通安全科技中心」(以下簡稱資安科技中心)。緣此,資通安全業務推動組織為資安會報、科技部及資安科

[2] 張裕榮,《國家資通安全科技中心設置條例草案評估報告》,立法院法制局法案評估報告,編號 970,103 年 9 月,頁 6。

技中心三級制。資安會報負責國家資通安全相關事項之政策，其幕僚作業由行政院資通安全辦公室辦理；科技部則為資通安全主管機關，負責資通安全政策之推動，並監督管理資安科技中心業務；資安科技中心負責提升國家資通安全防護能力，執行相關工作[3]。然「國家資通安全科技中心設置條例」於 105 年 5 月 3 日廢止，同年 5 月 25 日公布，其廢止理由為鑑於《國家資通安全科技中心設置條例》所列之資安中心業務範圍，其涉及國家資安政策規劃、設計、技術研發與執行等，實不應將原先資安會報、資安科技中心之資安二級管理制，降格為科技部、資安會報、資安中心之三級管理制；理應待三讀通過《資通安全管理法》(以下簡稱資安法)後，以較高層級、成立常設機構之方式，主管我國資通安全相關業務，爰廢止《國家資通安全科技中心設置條例》[4]。行政院遂於 105 年 8 月 1 日正式於院本部成立一個全新的資通安全處（以下簡稱資安處），由資安處負責國家所有的資安基本方針、政策及重大計畫、法規制定、通報應變和關鍵基礎設施的管理等事宜。

行政院為制定一部協助公務機關及受規範之非公務機關，認知自身資通安全風險並逐步提升自身資通安全能量之專法，遂成現階段建構、提升資通安全環境最有效率之規範面政策選擇。為達成上述目的，並使行政院統籌分配資源、整合民間力量，提升我國整體資通安全環境及資通安全意識，保障國家安全與公共利益，爰擬具「資通安全管理法草案」(以下簡稱本草案)，於 106 年 4 月 28 日以

[3] 立法院第 9 屆第 1 會期第 10 次會議議案關係文書，《行政院函送本院委員黃國昌等 11 人於第 9 屆第 1 會期第 4 次會議所提臨時提案之研處情形》，105 年 4 月 20 日，頁：報 1598。

[4] 立法院國會圖書館法律系統，「國家資通安全科技中心設置條例」廢止理由，http://lis.ly.gov.tw/lglawc/lawsingle?000742D7BB780000000000000000050000000000B000000^02822105050300^00123001001，參閱日期 106 年 5 月 31 日。

院臺護字第 1060172497 號函轉本院審議。

貳、立法要點

本草案要點如次[5]：

一、本法之立法目的及用詞定義。（草案第 1 條及第 2 條）

二、政府應整合民間力量推動資通安全相關事項。（草案第 3 條）

三、行政院應規劃及推動國家整體資通安全政策等事宜、公告國家資通安全情勢報告及資通安全發展方案；並得委任或委託其他公務機關、法人或團體辦理資通安全相關事務。（草案第 4 條及第 5 條）

四、行政院應訂定資通安全責任等級分級辦法，並得稽核非公務機關之資通安全維護情形；受稽核機關應就缺失或待改善事項完成改善報告，送交行政院、中央目的事業主管機關或直轄市、縣（市）政府。（草案第 6 條）

五、行政院應建立資通安全情資分享機制，並訂定相關事項之辦法。（草案第 7 條）

六、公務機關及非公務機關，於本法適用範圍內，委外辦理資通系統或資通服務事宜時，應就受託者之資通安全維護為監督。（草案第 8 條）

七、公務機關應考量其所屬資通安全責任等級之要求及保有或處理之資訊種類等條件，訂定、修正及實施資通安全維護計畫，並向上級或監督機關提出該計畫之實施情形。（草案第 9 條及第 11 條）

[5] 同註 1，修正草案總說明。

八、公務機關應由其首長指派副首長或適當人員擔任資通安全長，負責推動及監督機關內資通安全相關事務。（草案第 10 條）

九、公務機關應稽核其所屬或監督機關之資通安全維護計畫實施情形；受稽核機關應就缺失或待改善事項完成改善報告，送交稽核機關及上級或監督機關。（草案第 12 條）

十、公務機關應訂定資通安全事件之通報及應變機制，於知悉事件時，向上級機關、監督機關或行政院通報，並分別向上級機關、監督機關或行政院提出事件之調查、處理及改善報告。（草案第 13 條）

十一、公務機關所屬人員就資通安全維護之獎懲。（草案第 14 條）

十二、中央目的事業主管機關或直轄市、縣（市）政府應指定關鍵基礎設 施提供者，報請行政院核定。關鍵基礎設施提供者應訂定、修正、實 施資通安全維護計畫，並向中央目的事業主管機關或直轄市、縣（市）政府提出該計畫之實施情形；如經稽核發現缺失，應提出改善報告送 交中央目的事業主管機關或直轄市、縣（市）政府。（草案第 15 條）

十三、關鍵基礎設施提供者以外之非公務機關，應訂定、修正、實施資通 安全維護計畫；中央目的事業主管機關或直轄市、縣（市）政府得要求該等非公務機關提出計畫實施情形，並得進行稽核，發現有缺失者，應要求受稽核機關提出改善報告。（草案第 16 條）

十四、非公務機關應訂定資通安全事件之通報及應變機制，於知悉事件時向中央目的事業主管機關或直轄市、縣（市）政府通報，並應向中央目的事業主管機關或直轄市、縣（市）政府提出事件之調查、處理及改善報告；如為重大資通安全事件

者，其報告並應送行政院。行政院、中央目的事業主管機關或直轄市、縣（市）政府，於適當時機得公告與重大資通安全事件相關之必要內容及因應措施，並提供協助。（草案第17條）

十五、中央目的事業主管機關或直轄市、縣（市）政府因稽核資通安全維護計畫發現重大缺失，或遇重大資通安全事件，認有必要時，得進入受稽核或發生重大資通安全事件之非公務機關場所檢查；非公務機關及相關人員無正當理由不得規避、妨礙或拒絕；參與檢查之人 員就因而知悉之他人秘密資訊，應負保密義務。（草案第18條）

十六、非公務機關違反本法相關規定之罰則。（草案第19條至第21條）

叁、問題研析與建議

一、為使構成要件明確化，建議宜將關鍵基礎設施加以明確定義（草案第2條第1項第6款）

所謂國家關鍵基礎建設是指在一個國家中為維持國家安全、民生、經濟而提供的基本產品或服務，包含維持國家最起碼的經濟、民生、政府運作與國家安全息息相關的實體和以資訊電子為基礎的運作系統。常見的關鍵基礎設施包括公民營的電信、能源、銀行、財金、交通、供水及防救災等系統[6]。國家關鍵基礎設施脆弱度評估

[6] 方鴻春，「我國關鍵基礎建設安全防護」，《清流月刊》，98年2月號，http://www.mjib.gov.tw/FileUploads/eBooks/a7d057a843434ac1a4a44eaf53f4bd2c/Book_file/4843f93495f246b1854bd1054e4a7211.pdf，參閱日期106年5月4日。

與風險分析之運用，已成為許多國家重視的議題與重要工具；如果關鍵基礎設施之定義不清或意義不明確，亦或分類不明，可能導致無法有效運用有限的國家資源，作為國家關鍵基礎設施的保護策略指導方針。各國家關鍵基礎設施部門(如交通部、經濟部等)需要對資產的重要性，有精準而明確的定義，方可掌握需保護的資產項目及保護之程度性。各部門國家關鍵基礎設施政策決策者，需針對模糊且多變的關鍵基礎設施與資產清單，反覆的進行討論與辯論。因此，如何設定明確的資產重要性及判斷標準，是政府機關的當務之急，以利未來落實國家關鍵基礎設施相關安全法規與應變組織的訂定[7]。

行政院資安處表示，8 大資安旗艦計畫（詳如下表）將是年度資安計畫的基礎，透過強化關鍵基礎設施的資安防護措施，進一步達到提升整體國家資安防護能力。其中，與關鍵基礎設施相關的主管機關都必須在今年度，擇一完成包括「資安資訊分享與分析中心」、「資安監控中心」或者是「電腦緊急應變中心」重要的資安資料蒐集與分析平臺[8]。

[7] 黃俊能，《國家關鍵基礎設施防護之推動與策略－脆弱度評估與風險思維》，ithomew－臺灣資安大會－關鍵基礎建設安全論壇，https://cyber.ithome.com.tw/2017/forum5，參閱日期 106 年 5 月 12 日。

[8] 黃彥棻，「尋找臺灣資安新動能系列報導（一）：2017 年政府資安預算編列 25 億元，歷年最高」，《資安周報第 56 期》，106 年 1 月 4 日，http://www.ithome.com.tw/news/110923，參閱日期 106 年 5 月 10 日。

2017年政府8大資安旗艦計畫

部會	計畫名	計畫重點
經濟部	國防資安產業推動暨關鍵設施(水資源、民營能源)資安強化旗艦計畫	1. 建立水資源、能源領域ISAC。 2. 培育、輔導國內資安產業發展與高階資安專業人才養成。
科技部	資安前瞻創新研發計畫	1. 建立科學園區領域ISAC。 2. 補助大專院校投入先進資安技術研究與專業人才培育。
衛福部	關鍵基礎設施資安資訊分享與分析中心建置計畫	建立衛生關鍵基礎設施領域ISAC。
內政部	預防暨打擊科技犯罪精進刑事科技能量計畫	針對科技犯罪提升資安鑑識能量。
教育部	臺灣學術網路資安磐石計畫	建立臺灣學術網路資安訊息分析系統及建置防火牆聯合防禦架構系統，提升網路資訊安全。
交通部	關鍵基礎設施資安資訊分享與分析中心建置計畫	建立交通關鍵基礎設施領域ISAC。
通傳會	數位匯流/IoT資安威脅防禦機制暨資安實驗室建置與服務	國家基礎通訊網路防禦與IoT之資訊安全整體研究。
院資安處	國家資安防護前導計畫	研訂數位時代資安政策、法規及標準、發展國家資安風險評估機制、開展多層次與多邊國際合作關係、推廣資安認知方面訂定工作計畫。

資料來源：行政院資安處，2017年1月

關鍵基礎設施提供者如屬非公務機關，倘未依照本草案之規定，除令限期改正外，並可處以罰鍰等之行政裁罰，顯見關鍵基礎設施為重要之構成要件，宜加以明確定義；草案之定義雖為「國家關鍵基礎設施安全防護指導綱要」所對於關鍵基礎設施之定義，惟此為原則性或抽象式之概括規定，民間團體曾建言關鍵基礎設施定義需更清楚，許多企業對於非公務機關納管範圍，究竟包含哪些產業別，疑慮最深。基於法律之位階與明確性，尤其是訂有罰則之法律，宜將與當事人重要權益且必須之要件直接於資安法中明列規範，既可強化其位階性，且符合法律保留原則，有利於法律之明確性；故建議宜將關鍵基礎設施分類之第一層主部門分為能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院、中央與地方政府機關、

高科技園區等 8 類在定義中明確敘明[9]，將關鍵基礎設施安全防護之範圍予以明確規定。行政院雖考量關鍵基礎設施因應環境與時代變遷其範圍可能調整，然「國家關鍵基礎設施安全防護指導綱要」係每 2 年定期檢視調整，關鍵基礎設施之範圍亦可配合修正調整，並由行政院公告之即可。爰建議修正本草案第 2 條第 1 項第 6 款：「關鍵基礎設施：指能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院、中央與地方政府機關、高科技園區等部門之實體或虛擬資產、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，並經行政院公告者。」

二、為求法律文字表達精簡，建議刪除「依第十五條第一項規定」文字（草案第 2 條第 1 項第 7 款）

經查本草案第 15 條第 1 項規定：「中央目的事業主管機關或直轄市、縣（市）政府應指定關鍵基礎設施提供者，並報請行政院核定之。」與本草案第 2 條第 1 項第 7 款之「經中央目的事業主管機關或直轄市、縣（市）政府指定，並報行政院核定之非公務機關。」之語意相同，為求法律文字表達精簡，建議將「依第十五條第一項規定」之文字予以刪除。爰建議修正本草案第 2 條第 1 項第 7 款：「關

[9] 行政院，《國家關鍵基礎設施安全防護指導綱要》，103 年 12 月 29 日，頁 6。關鍵資訊基礎設施係指涉及核心業務運作，為支持關鍵基礎設施持續營運所需之重要資訊系統或調度、控制系統，亦屬關鍵基礎設施之重要元件，應配合對應之關鍵基礎設施統一納管。我國關鍵基礎設施分類，採三層架構。第一層為主部門，第二層為次部門，第三層為重要元件設施：(1)主部門：分為能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院、中央與地方政府機關、高科技園區等八類。(2)次部門：依主部門重要元件之屬性再區分次部門，例如能源主部門下再區分電力、石油、天然氣、化學與核能材料等次部門。(3)重要元件設施：係指維持設施營運所必須之重要設備、運作系統、通訊系統、維安系統，以及重要資訊系統或控制、調度系統等。

鍵基礎設施提供者：指維運或提供關鍵基礎設施之全部或一部，經中央目的事業主管機關或直轄市、縣（市）政府指定，並報行政院核定之非公務機關。」

三、為求語意明確，建議增列重大資安事件之定義（草案第 2 條第 1 項第 8 款）

本草案第 18 條條文提及重大缺失、重大資通安全事件，然何謂「重大」?若不加以明確定義，每個人認知程度不同，嗣後如何認定恐將引起爭議，民間團體亦曾建言應明訂重大資通安全事件之定義，基於法律優位及明確原則宜加以詳細說明以利遵循；雖行政院表達如「重大資安事件」…等部分用詞，會在子法中訂定[10]，然依中央法規標準法第 5 條規定：「左列事項應以法律定之：一、憲法或法律有明文規定，應以法律定之者。二、關於人民之權利、義務者。三、關於國家各機關之組織者。四、其他重要事項之應以法律定之者。」及同法第 6 條規定：「應以法律規定之事項，不得以命令定之。」，係為法律保留原則，重大資安事件屬重要事項宜由法律規定。建議增列本草案第 2 條第 1 項第 8 款：「重大資安事件：指國家機密資料遭洩漏、密級或敏感資料遭洩漏、關鍵資訊基礎設施系統或資料遭嚴重竄改、關鍵資訊基礎設施運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。」

四、資通安全政策攸關國家安全，建議每 2 年公布國家資通安全情勢報告及資通安全發展方案，以符現況所需與保持彈性（草案第 4 條）

依據世界經濟論壇發表的《2017 年全球風險報告》，2016 年的

[10] 行政院，《行政院法案及性別影響評估檢視表》，陸、徵詢及協商程序之附表－14、其他事項之參採與否及其理由，105 年 12 月 2 日，頁 19。

破壞性政治事件和社會動盪可能會給企業帶來巨大的營運和策略風險。報告的主要內容包括：（一）經濟問題是不穩定的根本原因：發達的經濟體正面臨經濟增長停滯和巨大的生產力挑戰，而新興市場正在經歷衰退和財政高度脆弱。（二）技術變革亟需管理：破壞的速度並不穩定，人工智能因為具有影響保密和安全後果的決策力而呈現出特定的風險。網絡攻擊持續關注關鍵的基礎設施以及商業公司，並且越來越廣泛地被國家和恐怖分子用來攻擊他們的對手。（三）政治關係緊張：公眾對政治領袖支持率低迷，黨派政治制度受挫，人民對現狀不滿情緒高漲。（四）全球合作備受壓力：國內焦慮加劇了地緣戰略競爭。發達經濟體希望加強邊境管制，而氣候變化改革充滿不確定性，貿易協定面臨崩潰[11]。由上可看出關鍵基礎設施是網路持續攻擊的關注對象之一，故如何管理新興科技是現今的一大考驗，若以嚴格的政策規範，將有可能延遲技術發展或阻礙了發展的潛力；但若沒有明確的制度，投資者將會因為擔心之後管理成效不佳，而使技術遭到濫用或失去民眾信心，而不敢投資。理想情況下，管理制度須保持其穩定性、可預測性、並且透明化，以建立投資者、公司、科學家等的信心，並讓大眾能產生一定程度的信任去評估早期負面成果報告。但管理制度也須保持彈性且具有足夠的適應性，並和快速變遷的技術發展保持良好的相容性。技術與技術相互碰撞、或是原有技術提供其他領域技術新平台，都將帶來發展的全新可能性[12]。

---

[11] 達信台灣（MARSH），《觀察 2017 年全球風險報告》，106 年 1 月 23 日，http://asia.marsh.com/taiwan/%E8%A7%80%E5%AF%9F%E8%88%87%E8%A7%A3%E6%B1%BA%E6%96%B9%E6%A1%88/ThoughtLeadership/ID/47172/2017.aspx，參閱日期 106 年 5 月 15 日。

[12] 科技產業資訊室（iKnow ）張小玫、杜君妮，《世界經濟論壇(WEF)發佈「全球風險報告」》，106 年 2 月 8 日，http://iknow.stpi.narl.org.tw/Post/Read.aspx?PostID=13172，參閱日期 106 年 5 月 12 日。

草案第 4 條規定行政院應定期公布國家資通安全情勢報告及資通安全發展方案，於其說明二：「為使各界了解國家資通安全趨勢，明定行政院應定期公布國家資通安全情勢報告，另配合國家資通安全政策之推動，原則以四年為一期，公布資通安全發展方案。」然資訊業務發展快速，4 年才公布一次似嫌過久，恐無法因應快速環境變化。資訊安全控制政策或原則應進行即時的評估，並定期審查政策或原則之可行性與有效性。資訊技術發展快速到超乎想像，制定相關規範性、僵化性之法規，應特別謹慎為之。如需要法律規範，速度要非常快速，如 2-3 年內無法制定完成，則往往大環境已經變化，可能原法規已經不再適用；如持續制定，反而會造成推動阻礙[13]。爰此，建議可配合「國家關鍵基礎設施安全防護指導綱要」每 2 年定期檢視調整，並同時公布國家資通安全情勢報告。爰建議修正本草案第 4 條：「行政院應規劃並推動國家資通安全政策、資通安全科技發展、國際交流合作及資通安全整體防護等相關事宜，並應每二年公布國家資通安全情勢報告及資通安全發展方案。」

五、為建立事權統一之管理機制，非公務機關資通安全維護計畫實施情形之稽核宜由中央目的事業主管機關擬訂，報請行政院核定之（草案第 6 條、第 15 條、第 16 條及第 19 條）

本草案第 6 條說明二：「為監督非公務機關實施資通安全維護計畫之情形，爰為第二項規定，並授權行政院訂定稽核頻率、內容與方法及其他相關事項之辦法。行政院依本項進行稽核時，應考量稽核對象之責任等級、其過往資通安全維護狀況、歷來接受行政院、

[13] VINCENT CHEN，《資訊發展與安全管理立法之觀察與建議》，105 年 9 月 6 日，https://rocket.cafe/talks/79059，參閱日期 106 年 5 月 10 日。

中央目的事業主管機關或直轄市、縣（市）政府稽核之頻率、結果及其他相關情形，決定最適之受稽核者名單。…」及說明三：「考量非公務機關依第二項規定接受稽核後，經發現其資通安全維護計畫實施有缺失或待改善情形，宜由行政院及相關機關進行監督，確認改善之狀況，爰為第三項規定。」然於本草案第 15 條說明四：「為確保資通安全維護計畫之落實，於第四項規定中央目的事業主管機關或直轄市、縣（市）政府應稽核所管關鍵基礎設施提供者之資通安全維護計畫實施情形。稽核時，宜考量受稽核者歷來接受行政院、中央目的事業主管機關或直轄市、縣（市）政府稽核之頻率與稽核結果等因素，決定最適之受稽核者名單與頻率。」及說明五：「第五項規定關鍵基礎設施提供者之資通安全維護計畫實施情形有缺失或待改善者，應提出改善報告，送交中央目的事業主管機關或直轄市、縣（市）政府，以確保資通安全維護計畫之落實。」，本草案第 16 條說明三：「考量資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，其內容宜有一致性，以利第一項之非公務機關適用與遵循，爰於第四項規定，由中央目的事業主管機關擬訂，並報請行政院核定之。」

本草案第 6 條係敘明非公務機關之資通安全維護計畫實施情形，行政院得稽核之，並授權行政院訂定稽核頻率、內容與方法及其他相關事項之辦法。但到本草案第 15 條及第 16 條卻為資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，由中央目的事業主管機關擬訂，報請行政院核定之。就文意來看似為行政院、中央目的事業主管機關、直轄市或縣（市）政府皆應稽核資通安全維護計畫，語意上似一再重複敘述，且稽核頻率不一由各自擬訂，是否會造成

非公務機關、關鍵基礎設施提供者受稽核頻率過高之疑慮，反而會降低配合意願。因資安人力資源欠缺是各單位相當困擾所在，應避免公務機關或是非公務機關承辦人員須經常提交報告之困擾，且為明確規範政府機關（構）資通安全責任等級分級作業流程，建議宜由中央目的事業主管機關、直轄市或縣（市）政府擬訂一套完善之資通安全維護計畫有關之必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，再報請行政院核定。

此外，本草案第 16 條係為規範關鍵基礎設施提供者以外之非公務機關之資通安全事項，依本草案第 2 條第 1 項第 5 款非公務機關指的是關鍵基礎設施提供者、公營事業及政府捐助之財團法人，故本草案第 16 條所規範的是公營事業及政府捐助之財團法人。然發現本草案第 15 條關鍵基礎設施提供者「應」向中央目的事業主管機關或直轄市、縣（市）政府提出資通安全維護計畫實施情形、中央目的事業主管機關或直轄市、縣（市）政府「應」稽核所管關鍵基礎設施提供者之資通安全維護計畫實施情形，使用的用語是「應」；惟本草案第 16 條卻為中央目的事業主管機關或直轄市、縣（市）政府「得」要求所管前項非公務機關，提出資通安全維護計畫實施情形、中央目的事業主管機關或直轄市、縣（市）政府「得」稽核所管第一項非公務機關之資通安全維護計畫實施情形，使用的用語是「得」。以正式之法律用語而言，「得」表非強制性之義務，行為人有選擇作為或不作為之自由；反之，如要表達強制之意時，正確之用語為「應」。建議本草案第 16 條既然規範的是公營事業及政府捐助之財團法人就更應要有強制性，況且資安法既已參考國際作法將關鍵基礎設施納入適用範圍，對於公營事業及政府捐助之財團法人

更不遑多讓，全國皆須符合一定標準以合乎整體國家資通安全之要求。

綜上，建議修正本草案第 6 條：「行政院應衡酌公務機關及非公務機關業務之重要性與機敏性、機關層級、保有或處理之資訊種類、數量、性質、資通系統之規模及性質等條件，訂定資通安全責任等級之分級；其分級基準、等級變更申請、義務內容、專責人員之設置及其他相關事項之辦法，由行政院定之。（第 1 項）中央目的事業主管機關、直轄市及縣（市）政府，應稽核非公務機關之資通安全維護計畫實施情形，行政院得稽核之；資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，由中央目的事業主管機關擬訂，報請行政院核定之。（第 2 項）非公務機關受前項之稽核，經發現其資通安全維護計畫實施有缺失或待改善者，應限期向中央目的事業主管機關或直轄市、縣（市）政府提出改善報告，如為重大資通安全事件者，並應送交行政院。（第 3 項）」及刪除本草案第 15 條第 4～6 項及第 16 條第 3、4 項。

爰上，建議修正本草案第 15 條：「中央目的事業主管機關或直轄市、縣（市）政府應指定關鍵基礎設施提供者，並報請行政院核定之。（第 1 項）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，並考量其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。（第 2 項）關鍵基礎設施提供者應向中央目的事業主管機關或直轄市、縣（市）政府提出資通安全維護計畫實施情形。（第 3 項）」及第 16 條：「關鍵基礎設施提供者以外之非公務機關，應符合其所屬資通安全責任等級之要求，並考量其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。(第 1 項) 中央目的事業主管機關或直轄市、縣（市）政府應要求所管前項非公務機關，提出資通安全維護計畫實施情形。(第 2 項)」此外，為配合刪除本草案第 15 條第 6 項及第 16 條第 4 項，建議修正本草案第 19 條：「…一、違反第六條第二項所定辦法中有關資通安全維護計畫必要事項之規定，或未依第十五條第二項或第十六條第一項規定，訂定、修正或實施資通安全維護計畫。二、違反第六條第二項所定辦法中有關資通安全維護計畫實施情形提出之規定，或未依第十五條第三項或第十六條第二項規定，向中央目的事業主管機關或直轄市、縣（市）政府提出資通安全維護計畫之實施情形。三、違反第六條第二項所定辦法中有關改善報告提出之規定，或未依第六條第三項規定，提出改善報告送交行政院、中央目的事業主管機關或直轄市、縣（市）政府。…。」

六、公務機關尤其應該重視資通安全風險，以提升資通安全能量；建議納入「年度評估報告」，以加強系統化資通安全風險管理（草案第 11 條）

本法草案最重要之立法目的在於「建構國家資通安全環境，以保障國家安全」，因此亟須加強系統化資通安全風險管理，以消弭破壞資通安全之因素或削弱其影響力至可接受之範圍。公務機關尤其應該重視資通安全風險，提升資通安全能量；先進國家有關資通安全的專法之規定內容，例如美國「聯邦資訊安全現代法」(Federal Information Security Modernization Act of 2014)[14]有關年度獨立評估

[14] https://www.congress.gov/bill/113th-congress/senate-bill/2521/text?overview=closed，參閱日期 106 年 6 月 15 日。

報告，即相當值得我們參考借鏡。茲將該法年度獨立評估報告相關規定重點，概要整理如後：

（一）每個機關每年應為其資通安全計畫及執行情形進行獨立評估，以便確認該機關的計畫及執行之有效性；所進行的評估應該包括：1.測試該機關資通安全的政策、程序及執行之有效性;2.評估該機關資通安全計畫的政策、程序及作法之有效性;3.衡酌該機關資通安全計畫與國家整體資通安全之關係。

（二）應由獨立的審核員進行審核，必要時由機關外部的審核員進行審核，即聘請獨立的機關外部審核員對計畫及其執行進行評估。

（三）對於運作或操控國家安全體系之機關，所進行的評估應確保運用適當方式並符合法律規定，以保護資通安全疏漏之風險。

（四）此評估可以基於該機關之資通安全計畫及其執行。

（五）此評估如涉及國家安全體系，提交的評估應包含摘要及相關於國家安全體系之部分。

（六）機關應採取適當措施確保資訊受保護，如果該資訊被揭露可能不利於資訊安全，而資訊保護措施應與風險程度應相符合，並遵守所有適用法規。

（七）提交國會之報告，應摘要資通安全涉及國家安全體系之部分，並確保資通安全體系的資訊安全，而資訊保護措施應與風險程度相符合，並遵守所有適用法規。資通安全計畫應定期進行評估，並向國會報告。

綜上所述，美國「聯邦資訊安全現代法」有關年度獨立評估報告之立法政策值得我們參採，故建議修正草案第 11 條：「公務機關

應每年向上級或監督機關提出資通安全維護計畫實施情形及年度評估報告；無上級機關者，其資通安全維護計畫實施情形應送交行政院。」

七、草案既有罰則之專章，建議將公務機關所屬人員之懲戒與懲處改列至罰則專章（草案第 14 條第 2 項改列為第 19 條）

本草案第 14 條係將公務機關所屬人員對於資通安全管理之獎勵、懲戒與懲處，列於本草案第 2 章之公務機關資通安全管理，然於本草案第 4 章罰則之第 19～21 條皆為非公務機關違反資通安全之處罰，此易造成罰則僅針對非公務機關而不處罰公務機關所屬人員之誤解，故建議宜將草案中有關之罰則統一規定於專章內，以示明確與一致。爰建議修正本草案第 14 條：「公務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。」本草案原第 14 條第 2 項改列為第 19 條，以下條次遞增。

八、重大資通安全事件之公告時間應明確且快速，以避免不確定性及延誤時效（草案第 17 條第 5 項）

為有效掌握我國政府機關（構）及公民營事業之資通訊系統遭受破壞、不當使用等資通安全事件，能迅速雙向通報及緊急應變處置，並在最短時間內回復，以確保國家利益與政府之正常運作[15]，已訂有「國家資通安全通報應變作業綱要」，現更於本草案內明確律定資通安全事件通報應變機制。考量重大資通安全事件可能影響多數人民之生命、身體或財產安全，宜由行政院、中央目的事業主管機關或直轄市、縣（市）

[15] 行政院國家資通安全會報，《國家資通安全通報應變作業綱要》，105 年 8 月 1 日，頁 2。

政府於知悉後，分別或共同公告必要之內容（例如發生原因、影響程度及目前控制之情形等）及因應措施，並提供相關協助，以利防範、避免損害之擴大[16]。然本草案第 17 條第 5 項僅規範於「適當時機」得公告與事件相關之必要內容及因應措施，並無明確之時間，未明文規範恐形成認知上之不同，為求明確與嚴謹，宜盡量避免解釋上可能產生歧異之用字或句法；為使文義明確，須在一定時間內將問題癥結查明，且因考量資訊技術發展快速，為爭取時效，爰建議宜訂為 1 個月內公告，使各單位對類此事件有所警惕與防範。建議修正本草案第 17 條第 5 項：「知悉重大資通安全事件時，行政院、中央目的事業主管機關或直轄市、縣（市）政府，於 1 個月內得公告與事件相關之必要內容及因應措施，並得提供相關協助。」

九、進入非公務機關場所檢查，其程序應更嚴謹與完備，以符合正當法律程序原則，避免造成侵權之虞（草案第 18 條第 1 項）

依中華民國憲法第 22 條：「凡人民之其他自由及權利，不妨害社會秩序、公共利益者，均受憲法之保障。」及第 23 條：「以上各條列舉之自由權利，除為防止妨礙他人自由、避免緊急危難、維持社會秩序或增進公共利益所必要者外，不得以法律限制之。」此分別為對基本人權之保障與限制之規範。本草案第 18 條為落實非公務機關資通安全之維護，並強化中央目的事業主管機關與直轄市、縣（市）政府之權責，於稽核資通安全維護情形發現有必要時，得派員攜帶執行職務證明文件，進入非公務機關場所檢查，然此舉卻為本草案爭點所在。依大法官解釋釋字第 603 號之解釋文：「…隱私權雖非憲法明文列舉之權利，惟基於人性

[16] 同註 1，條文對照表之第 17 條說明 3。

尊嚴與個人主體性之維護及人格發展之完整，並為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，隱私權乃為不可或缺之基本權利，而受憲法第 22 條所保障（本院釋字第五八五號解釋參照）。其中就個人自主控制個人資料之資訊隱私權而言，乃保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權。惟憲法對資訊隱私權之保障並非絕對，國家得於符合憲法第 23 條規定意旨之範圍內，以法律明確規定對之予以適當之限制。…」隱私權雖係基於維護人性尊嚴與尊重人格自由發展而形成，惟其限制並非當然侵犯人性尊嚴。憲法對個人資訊隱私權之保護亦非絕對，國家基於公益之必要，自得於不違反憲法第 23 條之範圍內，以法律明確規定強制取得所必要之個人資訊[17]。本草案第 18 條與上揭憲法維護人民資訊隱私權之本旨雖有未合，恐難以符合比例原則之要求，致侵害人民受憲法第 22 條保障之資訊隱私權；然依法律合憲性解釋原則，倘依憲法第 23 條為防止妨礙他人自由、避免緊急危難、維持社會秩序或增進公共利益所必要者，不得以法律限制。資通安全事件常關係國家安全及社會公共利益，得以法律或法律明確授權之命令加以限制，未構成違憲，只是應探究進入非公務機關場所檢查之手段是否合乎憲法比例原則之要求。然必須考慮者在於，資安的專業性以及其中涉及業者的營業秘密與相關智慧財產權等，其稽核的方法、手段、頻率乃至於派員檢查之相關程序究竟應如何規定，亦為政府所必要多加考量者。現行草案中關於稽核程序均由行政機關加以規定，而派員檢查之相關規定亦僅有一條文規範，顯然

[17] 司法院大法官解釋釋字第 603 號，94 年 9 月 28 日，http://www.judicial.gov.tw/constitutionalcourt/p03_01.asp?expno=603，參閱日期 106 年 5 月 25 日。

不足以保障業者於此可能受到的損害[18]。

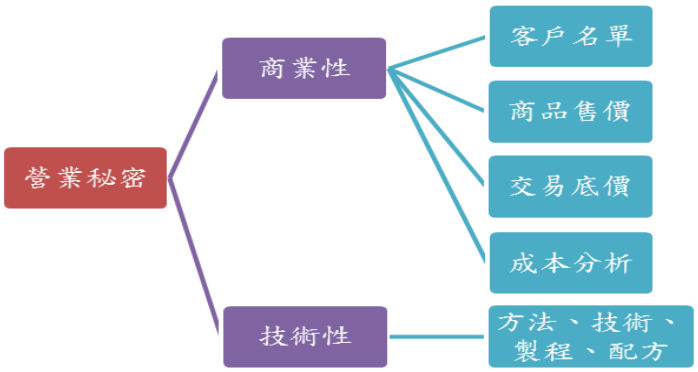
商業秘密（亦作營業秘密，俗稱商業機密）是指包括設計、程序、產品配方、製作方法、製作手工藝、管理訣竅、客戶名單或產銷策略等的技術信息和營業信息：且該信息不為普遍所知，能為權利人帶來經濟利益，具有現實的或潛在的實用性，並經權利人利用保密手段管理；同時該信息不與公共利益相衝突；作為商業秘密，通常需要如下構成要件：秘密性、新穎性、實用性及經濟價值性[19]。企業內部之營業秘密，可以概分為「商業性營業秘密」及「技術性營業秘密」二大類型（詳如圖二)。所謂「商業性營業秘密」，主要包括企業之客戶名單、經銷據點、商品售價、進貨成本、交易底價、人事管理、成本分析等與經營相關之資訊。所謂「技術性營業秘密」，顧名思義係指與特定產業研發或創新技術有關之機密，包括方法、技術、製程及配方等」基此，我國訂有營業秘密法。日前經濟部邀集產官學三方舉行「公司法」修法公聽會，討論公司法全盤修正修法委員會主張建置公司登記 E 化平台（草案第 388 條)，各方意見不一，企業擔心若把經營資訊上傳政府平台，可能有外洩風險。另外還有「產業創新條例部分條文修正草案」中對於法人科技專案的智慧財產流通運用時，除了要進行無形資產評價之外，更要求「將

[18] 盧映潔、林伯樺，《盧映潔觀點：「資通安全管理法草案」之修正建議》，風傳媒，106 年 5 月 15 日，http://www.storm.mg/article/264648，參閱日期 106 年 5 月 15 日。

[19] 維基百科，《商業秘密》，最後修訂於 105 年 1 月 29 日，https://zh.wikipedia.org/wiki/%E5%95%86%E4%B8%9A%E7%A7%98%E5%AF%86，參閱日期 106 年 5 月 18 日。18 世紀、19 世紀，商業秘密開始法律保護的進程。19 世紀中期，法國和德國的刑法懲處未經許可泄漏工廠秘密的行為。1820 年，英國衡平法院准許了一項使用泄漏商業秘密的禁令。1909 年德國制訂的《反不正當競爭法》，給予商業秘密司法救濟。20 世紀 50 年代以來，對商業秘密的保護進入專門立法保護與智慧財產權保護的並存階段。美國國家統一州法委員會於 1979 年制定了《統一商業秘密法》，英國下議院於 1981 年制定了《保護商業秘密權法》，1967 年簽訂的《成立世界智慧財產權組織公約》將「未公開的信息」納入智慧財產權範圍。1994 年在馬拉喀什通過的《與貿易有關的智慧財產權協定》明文把「商業秘密」列入一項與貿易有關的智慧財產權；同時認為它屬於「反不正當競爭」的一項內容，與《巴黎公約》中的反冒牌貨同屬一個條文管轄。

評價資料登錄於中央主管機關指定之資訊服務系統」(草案第 12 條第 2 項),也引發業者技術佈局機密洩漏的疑慮。上述兩項爭議顯示,為了因應數位經濟時代來臨,立法推動公司電子登記平台或是智慧財產評價資訊服務系統,確實是具有宣示政府去管制化及強化透明度決心的意義,堪稱立意良善。但是,該等立法除了應考量企業營運實務與法遵成本負擔之外,更不能忽略業者機密外洩的疑慮,而必須在資訊揭露與營業秘密保護間,找到適當的平衡點[20]。

圖二:營業秘密之分類



(經濟部智慧財產局,《營業秘密保護實務教戰手冊》,102 年 12 月,頁 5)

有論者主張稽核資通安全維護情形發現有必要時,得派員攜帶執行職務證明文件,進入非公務機關場所檢查,此檢查制度形同於刑事訴訟法中搜索扣押,有違憲之虞。另有論者主張此等稽核或派員檢查手段,對於民間業者之營業秘密保障有所侵害。對民間單位加以稽核或派員檢查,究竟在維護資通安全此等目的下,是否合乎於憲法比例原則之要求有所疑慮。對此等問題官方的回應方式如下:(一)刑事訴訟制度中的搜索與行政檢查有所不同,對於國民基本權之侵害有差異。現行法規中亦有如漁業法第 49 條、動物保護法第 23 條、職業安全衛生法第 36 條、

[20] 《莫因資訊揭露 衝擊企業營業秘密》,工商時報社論－火線焦點,106 年 5 月 31 日。

電業法第 67 條、稅捐稽徵法第 30 條、個人資料保護法第 22 條等行政檢查之規定。(二) 資安法草案中第 18 條規定，僅有於重大資通安全事件或因稽核發生重大缺失時，且認為有必要時方才派員檢查。固然行政檢查與搜索扣押之要件程序有別，且二者產生侵害之程度固然可能有異，但並無差異者在於其均對國民之基本權利產生侵害，因而其程序均應該依據法律明文規定為是，方合於憲法法治國原則之基本要求。然必須知道的是，對於此等資訊通訊產業而言，其資通安全之設計，例如程式碼設計或硬體配置等，與業者之智慧財產權與及營業方式具有高度相關，對於業者之財產權、隱私權以及營業自由等權利具有密切之關連，而行政單位要求其提出相關資訊時，對於業者之權利侵害不可謂之不巨大，且必須考慮資安的專業性以及其中涉及業者的營業秘密與相關智慧財產權等，其稽核的方法、手段、頻率乃至於派員檢查之相關程序究竟應如何規定，亦為政府所必要多加考量者[21]。持平而論，現行法規中已有許多關於行政檢查之規定（詳如表一），本草案第 18 條之規定並非首例，僅提供數個法規以供參考；惟因本草案牽涉資訊系統部分至為重要且敏感，對於非公務機關之資訊隱私、營業秘密及法遵成本亦應妥善加以考量。

表一：現行法規有關行政檢查之簡表

法規名稱及條次	法規內容
漁業法第 49 條	主管機關得派員至漁業人之漁船、漁業權漁場、陸上魚塭或其他有關場所，檢查其漁獲物、漁具、簿據及其他物件，並得詢問關係人；海岸巡防機關得依其職掌派員至漁業人之漁船檢查及詢問關係人。關係人均不得規避、妨礙或拒絕。…第一項人員於執行檢查時，應提示身分證明及指定

[21] 同註 18，http://www.storm.mg/article/264648，參閱日期 106 年 5 月 15 日。

	檢查範圍之機關證件；其未經提示者，被檢查人得拒絕之。
動物保護法第 23 條	…動物保護檢查員得出入動物比賽、宰殺、繁殖、買賣、寄養、展示及其他營業場所、訓練、動物科學應用場所，稽查、取締違反本法規定之有關事項。對於前項稽查、取締，不得規避、妨礙或拒絕。…動物保護檢查員於執行職務時，應出示有關執行職務之證明文件或顯示足資辨別之標誌；必要時，得請警察人員協助…。
職業安全衛生法第 36 條	中央主管機關及勞動檢查機構對於各事業單位勞動場所得實施檢查。其有不合規定者，應告知違反法令條款，並通知限期改善；…。
電業法第 67 條	主管機關對於電業設備及第三十條第一項規定之安全保護設施，得隨時查驗；其不合規定者，應限期修理或改換；如有發生危險之虞時，並得命其停止其工作及使用。發電業及輸配電業對於前項查驗，不得規避、妨礙或拒絕。
稅捐稽徵法第 30 條	稅捐稽徵機關或財政部賦稅署指定之調查人員，為調查課稅資料，得向有關機關、團體或個人進行調查，要求提示帳簿、文據或其他有關文件，或通知納稅義務人，到達其辦公處所備詢，被調查者不得拒絕。…。
個人資料保護法第 22 條	中央目的事業主管機關或直轄市、縣(市)政府為執行資料檔案安全維護、業務終止資料處理方法、國際傳輸限制或其他例行性業務檢查而認有必要或有違反本法規定之虞時，得派員攜帶執行職務證明文件，進入檢查，並得命相關人員為必要之說明、配合措施或提供相關證明資料。…中央目的事業主管機關或直轄市、縣(市)政府為第一項檢查時，得率同資訊、電信或法律等專業人員共同為之。對於第一項及第二項之進入、檢查或處分，非公務機關及其相關人員不得規避、妨礙或拒絕。參與檢查之人員，因檢查而知悉他人資料者，負保密義務。
大眾捷運法第 36 條	大眾捷運系統運輸上必要之設備，主管機關得派員檢查；設備不適當時，應通知其限期改正。
工程技術顧問公司管理條例第 22 條	主管機關得隨時派員檢查工程技術顧問公司之業務，或本條例所定該公司及其執業技師應遵守之事項；檢查時，並得令其提出證明文件、表冊及有關資料；工程技術顧問公司及其執業技師不得規避、妨礙或拒絕。
公司法第 21 條	主管機關得會同目的事業主管機關，隨時

	派員檢查公司業務及財務狀況，公司負責人不得妨礙、拒絕或規避。…主管機關依第一項規定派員檢查時，得視需要選任會計師或律師或其他專業人員協助辦理。
化粧品衛生管理條例第 25 條	國外輸入或國內產銷之化粧品及化粧品色素，直轄市或縣 (市) 衛生主管機關得派員持憑證明文件，赴各廠商抽查或檢查；必要時，得以原價抽取樣品，檢查其品質，廠商不得無故拒絕。中央衛生主管機關於必要時，得為前項之抽查或檢查，廠商不得無故拒絕。
化粧品衛生管理條例第 26 條	直轄市或縣 (市) 衛生及工業主管機關，應派員持憑證明文件，赴各化粧品及化粧品色素製造、加工之場所、倉庫、販賣處所，實地檢查其設備、裝置、製造程序、環境衛生及其成品、半成品、原料、配料、包裝、容器、標籤、仿單等，廠商不得無故拒絕。中央衛生及工業主管機關於必要時，得為前項之檢查，廠商不得無故拒絕。
天然氣事業法第 48 條	公用天然氣事業應定期檢查家庭、商業及服務業用戶之管線，並記載其結果；如不合規定，應通知用戶限期改善；其經用戶請求檢查者，亦同。用戶拒絕接受前項檢查，公用天然氣事業於認定有供氣安全之虞時，得報經直轄市、縣（市）主管機關同意，會同相關機關人員進行強制檢查。…第一項檢查人員及前項受委託辦理檢查之人員，於進行檢查相關業務時，應主動出示身分證明文件。…。
水污染防治法第 26 條	各級主管機關得派員攜帶證明文件，進入事業、污水下水道系統或建築物污水處理設施之場所，為下列各項查證工作：…。各級主管機關依前項規定為查證工作時，其涉及軍事秘密者，應會同軍事機關為之。對於前二項查證，不得規避、妨礙或拒絕。檢查機關與人員，對於受檢之工商、軍事秘密，應予保密。
水利法第 93 條之 6	主管機關或水利機關為執行有關水權、河川、排水、海堤、水庫、水利建造物、地下水鑿井業或用水計畫之管理，認有違反本法禁止或限制規定或有隱匿用水量逃漏耗水費之虞時，得派員進入事業場所、建築物或土地實施檢查，並得令相關人員為必要之說明、配合措施或提供相關資料；被檢查者不得規避、妨礙或拒絕。有具體事實足認有違反實施檢查之行為且規避、妨礙或拒絕檢查時，主管機關或水利機關得強制進入；必要時，並得商請轄區內警察機關協助之。實施前項檢查時，應先通知或公告。但有妨礙檢查目的之虞

	者，不在此限。第一項規定之檢查人員於執行檢查職務時，應主動出示執行職務證明文件或顯示足資辨別之標誌，並不得妨礙該場所正常業務之進行。第一項規定之檢查機關及人員，對於被檢查者之私人、工商秘密，應予保密。…。
民用航空法第 7 條之 1、23 條、23 條之 2、27 條、28 條之 1、40 條、41 條之 1、57 條、69 條、78 條、99 條之 7	均有規定民航局應（得）派員檢查從事自用航空器飛航活動者之各項人員、設備、飛航作業及活動，航空產品與其各項裝備及零組件製造廠、維修廠、民用航空人員訓練機構…等等，受檢者不得規避、妨礙或拒絕，檢查結果發現有缺失者，應通知其限期改善。
再生水資源發展條例第 16 條	直轄市、縣（市）主管機關或特定園區目的事業主管機關為執行再生水經營業各開發案及依第十一條第一項規定許可取用案之管理，得派員進入事業場所、設施範圍，實施各種工程設施、水質、水量等有關資料及紀錄之檢查，並得令相關人員為必要之說明、配合措施或提供相關資料；被檢查者及相關人員不得規避、妨礙或拒絕。前項規定之檢查人員於執行檢查職務時，應主動出示執行職務證明文件或足資辨別之標誌，並以不妨礙事業正常業務之進行為原則。第一項規定之檢查機關及人員，對於被檢查者之私人、工商秘密，應予保密。
再生能源發展條例第 18 條	中央主管機關於必要時，得要求再生能源發電設備設置者提供再生能源運轉資料，並得派員或委託專業機構查核；再生能源發電設備設置者不得規避、妨礙或拒絕。…；中央主管機關並得令其補充說明或派員檢查，自用發電設備設置者不得規避、妨礙或拒絕。…。
有限合夥法第 31 條	主管機關得會同目的事業主管機關，隨時派員檢查有限合夥之業務及財務狀況，有限合夥負責人不得規避、妨礙或拒絕。主管機關依前項規定派員檢查時，得視需要選任會計師、律師或其他專業人員協助辦理。
有線廣播電視法第 74 條	主管機關得派員攜帶證明文件，對系統實施檢查，…，籌設人或系統經營者不得規避、妨礙或拒絕。…。
投資經營非我國籍漁船管理條例第 7 條	…。主管機關於必要時，得派員對關係人、有關機關（構）或團體進行調查，並要求提示、交付非我國籍漁船投資經營之有關資料。前二項報告或調查遇有急迫情形時，主管機關得派員至有關處所實施檢查，並得詢問關係人。前三項執行之人員，應主動出示有關執行職務之證明文件

	或顯示足資識別之標誌。關係人或有關機關（構）、團體對於第一項至第三項之調查、檢查或提出報告、提示、交付有關資料之要求，不得規避、妨礙或拒絕。
災害防救法第 32 條	…。為執行依前項規定作成之處分，得派遣攜有證明文件之人員進入業者營業場所或物資所在處所檢查。
事業用爆炸物管理條例第 33 條	主管機關為防止災害得隨時派員檢查爆炸物製造、販賣或使用之工作場所安全設施、考核爆炸物管理及使用人員，並得向有關人員查詢簿、冊、書、表等紀錄。受檢查單位及有關人員對於前項檢查，不得規避、妨礙或拒絕。第一項檢查人員於執行檢查任務時，應主動出示其身分證件。
使用牌照稅法第 22 條	檢查人員執行職務時，應佩帶臂章。主管稽徵機關人員，應由各主管稽徵機關核發檢查證，以資證明。
社會救助法第 33 條	社會救助機構應接受主管機關派員對其設備、帳冊、紀錄之檢查。
空氣污染防制法第 43 條	各級主管機關得派員攜帶證明文件，檢查或鑑定公私場所或交通工具空氣污染物排放狀況、空氣污染收集設施、防制設施、監測設施或產製、儲存、使用之油燃料品質，並命提供有關資料。依前項規定命提供資料時，其涉及軍事機密者，應會同軍事機關為之。對於前二項之檢查、鑑定及命令，不得規避、妨礙或拒絕。…。
金融控股公司法第 52 條	…，主管機關得令金融控股公司及其子公司於限期內提供相關財務報表、交易資訊或其他有關資料，並得隨時派員，或委託適當機構，檢查金融控股公司或其子公司之業務、財務及其他有關事項。主管機關於必要時，得指定專門職業及技術人員為前項檢查事項，並向主管機關據實提出報告；…。
金融資產證券化條例第 105 條	主管機關得隨時派員或委託適當機構，就資產信託證券化計畫或資產證券化計畫之執行狀況及其他相關事項，檢查受託機構、特殊目的公司、創始機構、服務機構或其他關係人之業務、財務或其他有關事項，…。
保全業法第 13 條	主管機關得隨時派員攜帶證明文件，檢查保全業業務情形，並得要求其提供相關資料。保全業之董事、監察人、經理人或從業人員，對前項之檢查及要求，不得拒絕。…。
保險法第 148 條	主管機關得隨時派員檢查保險業之業務及財務狀況，或令保險業於限期內報告營業狀況。前項檢查，主管機關得委託適當機構或專業經驗人員擔任；其費用，由受

	檢查之保險業負擔。…
消防法第 14 條之 1	…主管機關派員檢查第一項經許可之場所時，應出示有關執行職務之證明文件或顯示足資辨別之標誌；管理權人或現場有關人員不得規避、妨礙或拒絕，並應依檢查人員之請求，提供相關資料。
海洋污染防治法第 6 條	各級主管機關、執行機關或協助執行機關，得派員攜帶證明文件，進入港口、其他場所或登臨船舶、海洋設施，檢查或鑑定海洋污染事項，並命令提供有關資料。…。對前二項之檢查、鑑定及命令，不得規避、妨礙或拒絕。…。

（資料來源：參閱全國法規資料庫後自行整理）

再者，有關得派員攜帶執行職務證明文件，進入非公務機關場所檢查，其檢查人員之資格應加以明確界定，因於本草案第 5 條規定行政院得委任或委託其他公務機關、法人或團體，辦理資通安全整體防護、國際交流合作及其他資通安全相關事務；本草案第 8 條規定公務機關或非公務機關可委外辦理資通系統之建置、維運或資通服務之提供，顯見辦理資通安全相關事務者並非全為公職人員，受委任或委託之非公職人員即使攜帶執行職務證明文件，進入非公務機關場所檢查，其身分及公信力仍值得商榷；故檢查人員之身分及資格宜詳加規範與斟酌，畢竟此與民眾之財產權、隱私權及營業秘密等權利影響甚鉅，應審慎為之；執行時應有具法律及其他專業之人員陪同，以維護基本人權及避免侵權。建議修正本草案第 18 條第 1 項:「中央目的事業主管機關或直轄市、縣(市)政府因稽核資通安全維護情形發現重大缺失，或遇重大資通安全事件，而認有必要時，得派員率同法律及其他專業人員，攜帶檢查證及執行職務證明文件，進入非公務機關場所檢查，並得命相關人員為必要之說明、配合措施或提供相關證明資料。」

十、法案性別與人權影響評估

經行政院聘請性平與人權專家審查本草案，認為本案內容並無以特定性別、性傾向或性別認同者為規範對象，且執行方式均不因性別、性傾向或性別認同不同而有差異，所規範對象及執行方式無差異，亦不會產生不同結果；在人權影響評估部分，經檢視本草案，符合憲法、國際規範、性別平等政策綱領等要求，並符合憲法有關人民權利之規定、公民與政治權利國際公約及經濟社會文化權利國際公約（詳如附錄二）。

肆、結論與建議

科技創新是未來經濟和社會發展之關鍵，網路資安風險複雜性越來越高，近來資安事件層出不窮且手法越見精進，資安法更顯重要。資安法為資安法制化之基礎，資通安全政策之推動所涉範圍甚廣，規範內容涉及民間業者，須落實「資安等於國安」的政策方針，方能有效規劃我國之資通安全管理政策，以建構安全之資通環境。

本報告針對本草案條文內容檢視後，並就其性別及人權影響評估結果加以檢視與分析，提出以下建議，以供委員問政及修法之參考：

一、為使構成要件明確化，建議宜將關鍵基礎設施加以明確定義（草案第 2 條第 1 項第 6 款）

二、為求法律文字表達精簡，建議刪除「依第十五條第一項規定」文字（草案第 2 條第 1 項第 7 款）

三、為求語意明確，建議增列重大資安事件之定義（草案第 2 條第 1 項第 8 款）

四、資通安全政策攸關國家安全，建議每 2 年公布國家資通安全情勢報告及資通安全發展方案，以符現況所需與保持彈性（草案第 4 條）

五、為建立事權統一之管理機制，非公務機關資通安全維護計畫實施情形之稽核宜由中央目的事業主管機關擬訂，報請行政院核定之（草案第 6 條、第 15 條、第 16 條及第 19 條）

六、公務機關尤其應該重視資通安全風險，以提升資通安全能量；建議納入「年度評估報告」，以加強系統化資通安全風險管理（草案第 11 條）

七、草案既有罰則之專章，建議將公務機關所屬人員之懲戒與懲處改列至罰則專章（草案第 14 條第 2 項改列為第 19 條）

八、重大資通安全事件之公告時間應明確且快速，以避免不確定性及延誤時效（草案第 17 條第 5 項）

九、進入非公務機關場所檢查，其程序應更嚴謹與完備，以符合正當法律程序原則，避免造成侵權之虞（草案第 18 條第 1 項）

伍、條文對照表

資通安全管理法草案條文對照表

行政院提案條文	本報告建議條文	說明
第一章　總則	（無修正意見）	章名。
第一條　為積極推動國家資通安全政策，加速建構國家資通安全環境，帶動資通安全產業發展，以保障國家安全，維護社會公共利益，特制定本法。	（無修正意見）	一、明定本法之立法目的。 二、隨著數位及其他資通科技（Information Communication Technology）應用之普及，資通安全議題日益受到重視。為有效規劃我國之資通安全管理政策，落實於公、私部門，以建構安全之資通環境，進而保障國家安全，維護社會公共利益，特制定本法。
第二條　本法用詞，定義如下： 一、資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。 二、資通服務：指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處	第二條　本法用詞，定義如下： 一、資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。 二、資通服務：指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處	**行政院說明：** 一、第一項明定本法用詞定義： （一）參考美國國家標準技術研究所（National Institute of Standards and Technology）SP800-60 Volume I:Guildfor Mapping Type of Information and Information System to

理、使用或分享相關之服務。 三、資通安全：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。 四、公務機關：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。 五、非公務機關：指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。 六、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	理、使用或分享相關之服務。 三、資通安全：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。 四、公務機關：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。 五、非公務機關：指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。 六、關鍵基礎設施：指<u>能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院、中央與地方政府機關、高科技園區等部門之</u>實體或虛擬	Security Categories 及經濟部標準檢驗局公布國家標準 CNS 27001「資訊技術-安全技術-資訊安全管理-要求事項」等文件，於第一款至第三款規定資通系統、資通服務及資通安全之定義。 （二）第四款及第五款規定公務機關及非公務機關。公務機關指依法行使公權力之中央、地方機關（構）或公法人，例如總統府、行政院、立法院、司法院、考試院、監察院、直轄市政府、縣（市）政府、公立社會教育機構、公立文化機構、公立醫療機構或行政法人等。另考量軍事機關及情報機關之性質特殊，其資通安全管理宜由該等機關另行規定，故定明非屬本法所稱公務機關；該等機關之範

有重大影響之虞，並經行政院公告者。 七、關鍵基礎設施提供者：指維運或提供關鍵基礎設施之全部或一部，依第十五條第一項規定經中央目的事業主管機關或直轄市、縣（市）政府指定，並報行政院核定之非公務機關。 前項第五款所稱政府捐助之財團法人，其範圍於施行細則中定之。	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，並經行政院公告者。 七、關鍵基礎設施提供者：指維運或提供關鍵基礎設施之全部或一部，經中央目的事業主管機關或直轄市、縣（市）政府指定，並報行政院核定之非公務機關。 八、重大資安事件：指國家機密資料遭洩漏、密級或敏感資料遭洩漏、關鍵資訊基礎設施系統或資料遭嚴重竄改、關鍵資訊基礎設施運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。	圍，將於施行細則中規範。非公務機關則包括關鍵基礎設施提供者、公營事業及政府捐助之財團法人。 （三）參考美國 31 CFR 800.208 所定關鍵基礎設施（critical infrastructure）、日本網路安全基本法（サイバーセキュリティ基本法）第三條所定重要社會基礎業者、韓國情報通信基礎保護法（정보통신기반보호법）第二條所定情報通信基礎設施等定義，於第六款明定關鍵基礎設施之內涵，並考量關鍵基礎設施因應環境與時代變遷，其範圍可能調整，故規定由行政院公告之。依據行政院訂定之「國家關鍵基礎設施安全防護指導綱要」，關鍵基礎設施之範圍分為能

	前項第五款所稱政府捐助之財團法人，其範圍於施行細則中定之。	源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院、中央與地方政府機關、高科技園區等八大功能領域，其下並各分為數項次領域及重要元件設施；因前揭指導綱要每兩年將定期檢視調整，關鍵基礎設施之範圍，亦將配合修正調整。 (四)考量關鍵基礎設施對國家安全、社會公共利益、國民生活及經濟活動有重大影響，然各維運關鍵基礎設施之非公務機關其屬性及重要性仍有不同，爰於第七款規定關鍵基礎設施提供者為由中央目的事業主管機關或直轄市、縣（市）政府指定其中具重要性者，並報行政院核定之非公務機關。 (五)提供或維運關鍵基礎設施之全部或一

		部者，如屬本法所定義之公務機關，應遵循本法有關公務機關之規定；至其他關鍵基礎設施之提供者，則應遵循本法有關關鍵基礎設施提供者之規定。 （六）非提供或維運關鍵基礎設施功能或重要元件設施，而僅提供關鍵基礎設施所需用之其他設備或服務者，雖非本法所稱關鍵基礎設施提供者，但如其係受關鍵基礎提供者委託辦理資通系統之建置、維運或資通服務之提供時，仍應依本法第八條規定，受委託者之監督。 二、有關本法規範之政府捐助之財團法人，其範圍宜與財團法人相關規定內涵一致，爰為第二項規定；未來將參考財團法人法草案第二條第二項及第三項規定，於施行細則中定明其範圍。

		本報告說明： 一、關鍵基礎設施提供者如屬非公務機關，倘未依照本草案之規定，除令限期改正外，並可處以罰鍰等之行政裁罰，顯見關鍵基礎設施為重要之構成要件，宜加以明確定義；基於法律之位階與明確性，尤其是訂有罰則之法律，宜將與當事人重要權益且必須之要件直接於資安法中明列規範，既可強化其位階性，且符合法律保留原則，有利於法律之明確性。 二、經查第十五條第一項規定:「中央目的事業主管機關或直轄市、縣（市）政府應指定關鍵基礎設施提供者，並報請行政院核定之。」與第二條第一項第七款之「經中央目的事業主管機關或直轄市、縣（市）政府指定，並報行政院核定之非公務機關。」之語意相同，為求法律文字表達精簡，建議將第

		一項第七款中之「依第十五條第一項規定」之文字予以刪除。 三、本草案第十八條提及重大缺失、重大資通安全事件，然何謂「重大」?若不加以明確定義，每個人認知程度不同，嗣後如何認定恐將引起爭議，民間團體亦曾建言應明訂重大資通安全事件之定義，基於法律優位及明確原則宜加以詳細說明以利遵循；雖行政院表達如「重大資安事件」…等部分用詞，會在子法中訂定，然依中央法規標準法第五條及第六條規定係為法律保留原則，重大資安事件屬重要事項宜由法律規定，爰建議增列。
第三條　為提升資通安全，政府應提供資源，整合民間及產業力量，提升全民資通安全意識，並推動下列事項： 一、資通安全專業人才之培育。	（無修正意見）	一、鑒於資通安全之提升須以全民重視為前提，並須佐以先進之資通安全技術、軟硬體、專業人才等資源，政府應與民間共同提升全民資通安全意識，推動資通安全產業，以利先進資通安

二、資通安全科技之研發、整合、應用、產學合作及國際交流合作之推動。 三、資通安全產業之發展及推動。 四、資通安全軟硬體技術規範、相關服務與審驗機制之發展及推動。		全技術、軟硬體、專業人才等之發展，爰參考日本網路安全基本法第十九條產業之振興及國際競爭力強化、第二十條研究開發之推動、第二十一條人才之確保等規定，為本條規範。 二、關於租稅優惠措施，因事涉國家稅收，且現行已有產業創新條例、科學技術基本法等法律相關規定可資運用，爰不另於本法規範，併予敘明。
第四條　行政院應規劃並推動國家資通安全政策、資通安全科技發展、國際交流合作及資通安全整體防護等相關事宜，並應定期公布國家資通安全情勢報告及資通安全發展方案。	第四條　行政院應規劃並推動國家資通安全政策、資通安全科技發展、國際交流合作及資通安全整體防護等相關事宜，並應每二年公布國家資通安全情勢報告及資通安全發展方案。	**行政院說明：** 一、考量我國有關資通安全政策之推動所涉範圍甚廣，為利相關業務之推動，爰明定行政院應考量國家資通安全相關事務發展之需求，規劃並推動國家資通安全政策、資通安全科技發展、國際交流合作及資通安全整體防護等相關事宜。 二、為使各界了解國家資通安全趨勢，明定行政院應定期公布國家資通安全情勢報告，另配合國

		家資通安全政策之推動，原則以四年為一期，公布資通安全發展方案。 **本報告說明：** 上述說明二:「為使各界了解國家資通安全趨勢，明定行政院應定期公布國家資通安全情勢報告，另配合國家資通安全政策之推動，原則以四年為一期，公布資通安全發展方案。」然資訊業務發展快速，四年才公布一次似嫌過久，恐無法因應快速環境變化；資訊安全控制政策或原則應進行即時的評估，並定期審查政策或原則之可行性與有效性。爰此，建議可配合「國家關鍵基礎設施安全防護指導綱要」每二年定期檢視調整，並同時公布國家資通安全情勢報告。
第五條　行政院得委任或委託其他公務機關、法人或團體，辦理資通安全整體防護、國際交流合作及其他資通安全相關事務。	（無修正意見）	一、除政策制定等本質上不宜委任或委託辦理之事務外，行政院為推動資通安全業務，如有需要，得依行政程序法第十五條或第十六條規定，委任或委託其他公務機關、法人或團體辦理。為利實務運作，爰為本

		條規範。又委外事務倘不涉及公權力之移轉，例如國際法規或國際政策之研析，或雖為資通安全整體防護或國際交流等事項而未有公權力移轉之情形時，則仍應依政府採購法等規定辦理。 二、行政院依本條規定為委任或委託，因涉及公權力之移轉，應考量事務之性質、對象之屬性等事項，先行評估委任或委託辦理之適當性後，再行為之。
第六條　行政院應衡酌公務機關及非公務機關業務之重要性與機敏性、機關層級、保有或處理之資訊種類、數量、性質、資通系統之規模及性質等條件，訂定資通安全責任等級之分級；其分級基準、等級變更申請、義務內容、專責人員之設置及其他相關事項之辦法，由行政院定	第六條　行政院應衡酌公務機關及非公務機關業務之重要性與機敏性、機關層級、保有或處理之資訊種類、數量、性質、資通系統之規模及性質等條件，訂定資通安全責任等級之分級；其分級基準、等級變更申請、義務內容、專責人員之設置及其他相關事項之辦法，由行政院定	**行政院說明：** 一、考量公務機關與非公務機關之規模及業務性質不一，其應遵行之資通安全責任等級亦應有不同，此外，資通安全責任等級宜因機關調整、裁撤、業務變動或運用之資通系統發生重大變更等事由，而有所調整，以達到資通安全防護之最適效果。就此，目前有「政府機關（構）資通安全責任等級分級

之。 行政院得稽核非公務機關之資通安全維護計畫實施情形；其稽核之頻率、內容與方法及其他相關事項之辦法，由行政院定之。 非公務機關受前項之稽核，經發現其資通安全維護計畫實施有缺失或待改善者，應向行政院提出改善報告，並送中央目的事業主管機關或直轄市、縣（市）政府。	之。 中央目的事業主管機關、直轄市及縣（市）政府，應稽核非公務機關之資通安全維護計畫實施情形，行政院得稽核之；資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，由中央目的事業主管機關擬訂，報請行政院核定之。 非公務機關受前項之稽核，經發現其資通安全維護計畫實施有缺失或待改善者，應限期向中央目的事業主管機關或直轄市、縣（市）政府提出改善報告，如為重大資通安全事件者，並應送交行政院。	作業規定」可作為遵循之參考；於資通安全管理法制化後，上述諸事宜亦應加以規定，爰於第一項明定行政院應衡酌公務機關及非公務機關業務等事項，訂定資通安全責任等級之分級，並就其分級基準、等級變更申請、義務內容及專責人員之設置及其他相關事項，授權該院訂定辦法規範。 二、為監督非公務機關實施資通安全維護計畫之情形，爰為第二項規定，並授權行政院訂定稽核頻率、內容與方法及其他相關事項之辦法。行政院依本項進行稽核時，應考量稽核對象之責任等級、其過往資通安全維護狀況、歷來接受行政院、中央目的事業主管機關或直轄市、縣（市）政府稽核之頻率、結果及其他相關情形，決定最適之受稽核者名單。至於公務機關資通安全維護計畫實施情

		形之稽核，則於第十二條規範。 三、考量非公務機關依第二項規定接受稽核後，經發現其資通安全維護計畫實施有缺失或待改善情形，宜由行政院及相關機關進行監督，確認改善之狀況，爰為第三項規定。 **本報告說明：** 一、第六條敘明非公務機關之資通安全維護計畫實施情形，行政院得稽核之，並授權行政院訂定稽核頻率、內容與方法及其他相關事項之辦法。但第十五條及第十六條卻為資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，由中央目的事業主管機關擬訂，報請行政院核定之。語意上似一再重複敘述，且稽核頻率不一由各自擬訂，是否會造成非公務機關、關鍵基礎設施提

		供者受稽核頻率過高之疑慮，反而會降低配合意願。因資安人力資源欠缺是各單位相當困擾所在，應避免公務機關或是非公務機關承辦人員須經常提交報告之困擾，且為明確規範政府機關（構）資通安全責任等級分級作業流程，建議宜由中央目的事業主管機關、直轄市或縣（市）政府擬訂一套完善之資通安全維護計畫有關之必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，再報請行政院核定。 二、另第十六條係為規範關鍵基礎設施提供者以外之非公務機關之資通安全事項，依草案第二條第一項第五款非公務機關指的是關鍵基礎設施提供者、公營事業及政府捐助之財團法人，故第十六條所規範的是公營事業及政府捐助之財

		團法人。然發現第十五條關鍵基礎設施提供者「應」向中央目的事業主管機關或直轄市、縣（市）政府提出資通安全維護計畫實施情形、中央目的事業主管機關或直轄市、縣（市）政府「應」稽核所管關鍵基礎設施提供者之資通安全維護計畫實施情形，使用的用語是「應」；惟第十六條卻為中央目的事業主管機關或直轄市、縣（市）政府「得」要求所管前項非公務機關，提出資通安全維護計畫實施情形、中央目的事業主管機關或直轄市、縣（市）政府「得」稽核所管第一項非公務機關之資通安全維護計畫實施情形，使用的用語是「得」。以正式之法律用語而言，「得」表非強制性之義務，行為人有選擇作為或不作為之自由；反之，如要表達強制之意時，正確之用語為「應」。建

		議第十六條既然規範的是公營事業及政府捐助之財團法人就更應要有強制性，況且資安法既已參考國際作法將關鍵基礎設施納入適用範圍，對於公營事業及政府捐助之財團法人更不遑多讓，全國皆須符合一定標準以合乎整體國家資通安全之要求。爰刪除刪除草案第十五條第四項至第六項及第十六條第三、四項，統一規定於第六條第三項。
第七條　行政院應建立資通安全情資分享機制。 前項資通安全情資之分析、整合與分享之內容、程序、方法及其他相關事項之辦法，由行政院定之。	（無修正意見）	一、為增進與改善我國境內面對資通安全威脅與風險之應變能力及策略擬定，應建立相關資通安全情資分享機制，爰為第一項規定。 二、第二項定明資通安全情資之分析、整合與分享之內容、程序、方法及其他相關事項之辦法，由行政院定之，以資遵循。
第八條　公務機關或非公務機關，於本法適用範圍內，委外辦	（無修正意見）	考量公務機關或非公務機關於本法適用範圍內委外辦理資通系統建置、維運或資通

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。		服務之提供時，應依所委外項目之性質與資通安全需求，選任適當之受託者，並就受託者之資通安全維護為監督，以確保國家安全、社會公共利益或個人權益，爰為本條規定。相關監督事項之技術性及細節性內容，將於施行細則中規定。
第二章　公務機關資通安全管理	（無修正意見）	章名。
第九條　公務機關應符合其所屬資通安全責任等級之要求，並考量其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。	（無修正意見）	一、為確保公務機關之資通安全，避免因人為疏失、蓄意或自然災害等風險，致機關資通系統或資訊遭不當使用、洩漏、竄改、破壞等情事，影響及危害機關業務，公務機關（包含總統府、行政院、立法院、司法院、考試院、監察院、直轄市政府、縣（市）政府與其所屬或監督之各級公務機關及直轄市議會、縣（市）議會等）應符合第六條第一項所定資通安全責任等級之要求，並考量其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，爰為本條規定。公務機關訂修及實施上開計畫，應衡酌機關資源之合理分配，並依循上級或監督機關之相關資通安全規定為之。 二、有關資通安全維護計畫之內容，將由行政院訂定範本，提供各公務機關參考，以利執行。
第十條　公務機關應置資通安全長，由機關首長指派副首長或適當人員兼任，負責推動及監督機關內資通安全相關事務。	（無修正意見）	為確保有效推動資通安全維護事項，公務機關應置資通安全長，由其成立相關推動組織及督導推動相關工作。考量資通安全長如由副首長擔任，更能提升資通安全於機關中之重要性，並參考美國二〇一四年聯邦資訊安全現代化法（Federal Information Security Modernization Act of 2014）§3554 關於資訊長應指定資深資安專責人員負責相應事務規定之意旨，爰為本條規定。
第十一條　公務機關應每年向上級或監	第十一條　公務機關應每年向上級或監	**行政院說明：** 參考日本網路安全基本法第

督機關提出資通安全維護計畫實施情形；無上級機關者，其資通安全維護計畫實施情形應送交行政院。	督機關提出資通安全維護計畫實施情形及年度評估報告；無上級機關者，其資通安全維護計畫實施情形應送交行政院。	十二條有關促進地方公共團體確保網路資訊安全相關事項之規定，及同法第三十條規定相關行政機關之首長應適時提供與網路資訊安全相關之資料或資訊，以利執行所掌事務之精神，明定公務機關應每年向上級或監督機關提出資通安全維護計畫實施情形，以確認其實施成效，並使上級或監督機關得了解及稽核所屬或受監督機關之年度資通安全維護情形。另因總統府、立法院、司法院、考試院、監察院、直轄市政府、縣（市）政府、直轄市議會及縣（市）議會等公務機關無上級機關，爰規定無上級機關者應將資通安全維護計畫實施情形送交行政院。行政院收受上開計畫實施情形後將予以備查，並得視情形提供必要協助。 **本報告說明：** 本草案最重要之立法目的在於「建構國家資通安全環境，以保障國家安全」，因此亟須加強系統化資通安全風險管理，以消弭破壞資通安全之因素或削弱其影響力至可

		接受之範圍。公務機關尤其應該重視資通安全風險，提升資通安全能量；先進國家有關資通安全專法之規定內容，例如美國「聯邦資訊安全現代法」有關年度獨立評估報告，值得我們參考借鏡。
第十二條　公務機關應稽核其所屬或監督機關之資通安全維護計畫實施情形。 受稽核機關之資通安全維護計畫實施有缺失或待改善者，應提出改善報告，送交稽核機關及上級或監督機關。	（無修正意見）	一、第一項規定公務機關應稽核其所屬或監督機關之資通安全維護計畫實施情形。各公務機關對於其所屬或監督之各級公務機關，應依其機關層級、業務及其他相關情形，就稽核之基準、頻率、內容與方法訂定相關行政規則，以利執行。稽核時，宜考量受稽核者歷來接受行政院、上級或監督機關稽核之頻率與結果等因素，決定最適之受稽核者。 二、第二項規定受稽核機關之資通安全維護計畫實施有缺失或待改善者，應向稽核機關及上級或監督機關提出改善報告，以確保資通安全維護計畫之落實及政府資通安全維護之強度。

第十三條　公務機關為因應資通安全事件，應訂定通報及應變機制。 公務機關知悉資通安全事件時，除應通報上級或監督機關外，並應通報行政院；無上級機關者，應通報行政院。 公務機關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，並送交行政院；無上級機關者，應送交行政院。 前三項通報及應變機制之必要事項、通報內容、報告之提出及其他相關事項之辦法，由行政院定之。	（無修正意見）	一、為即時掌控資通安全事件，並有效降低其所造成之損害，爰於第一項規定公務機關應建立資通安全事件之通報及應變機制。所稱資通安全事件，係指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，致有無法符合機密性、完整性及可用性之事件；其具體類型將於施行細則及本條第四項授權訂定之辦法中規範。 二、參考日本網路安全基本法第十八條政府相關組織就有重大網路安全影響之虞之事件有相互合作、分享資訊並採取必要措施之義務之規定，於第二項明定公務機關知悉資通安全事件時，除應通報上級或監督機關外，並應通報行政院。另因總統府、立法院、司法院、考試院、監察院、直轄市政府、縣（市）政府、直轄市議

		會及縣（市）議會等公務機關無上級機關，爰規定無上級機關者應通報行政院。 三、考量公務機關於知悉資通安全事件後，應進行調查、處理及改善工作，爰於第三項規定公務機關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，並送交行政院，以利上級機關、監督機關或行政院監督，並得據以提供必要之協助。 四、關於公務機關資通安全事件之通報及應變，目前有「國家資通安全通報應變作業綱要」可資遵循參考，於本法施行後，應檢視原有機制並依本法要求調整之，故第四項授權行政院訂定第一項至第三項通報及應變機制之必要事項、通報內容、報告之提出及其他相關事項之辦法，以利公務機關適用。
第十四條　公務機關所屬人員對於機關	第十四條　公務機關所屬人員對於機關	**行政院說明：** 公務機關所屬人員關於資通

之資通安全維護績效優良者，應予獎勵。 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。	之資通安全維護績效優良者，應予獎勵。	安全事務之獎懲本有公務人員考績法、公務員懲戒法等規定加以規範，惟為促進該等人員對於資通安全工作之重視與投入，爰為本條規定。公務機關所屬人員於踐行本法要求事項成果優良或卓越時，應予獎勵；如因故意或過失，未踐履本法所定資通安全義務時，應受懲戒或懲處；如有其他違反資通安全義務而涉及民事或刑事責任之情形時，仍應依各該相關法律處理之。 **本報告說明：** 第十四條係將公務機關所屬人員對於資通安全管理之獎勵、懲戒與懲處，列於第二章之公務機關資通安全管理，然於第四章罰則之第十九條至第二十一條皆為非公務機關違反資通安全之處罰，此易造成誤解為罰則僅針對非公務機關而不處罰公務機關所屬人員，故建議將罰則統一規定於專章內，以示明確與一致。
第三章　非公務機關資通安全管理	（無修正意見）	章名。
第十五條　中央目的	第十五條　中央目的	**行政院說明：**

事業主管機關或直轄市、縣（市）政府應指定關鍵基礎設施提供者，並報請行政院核定之。 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，並考量其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。 關鍵基礎設施提供者應向中央目的事業主管機關或直轄市、縣（市）政府提出資通安全維護計畫實施情形。 中央目的事業主管機關或直轄市、縣（市）政府應稽核所管關鍵基礎設施提供者之資通安全維護計畫實施情形。 關鍵基礎設施提供者之資通安全	事業主管機關或直轄市、縣（市）政府應指定關鍵基礎設施提供者，並報請行政院核定之。 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，並考量其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。 關鍵基礎設施提供者應向中央目的事業主管機關或直轄市、縣（市）政府提出資通安全維護計畫實施情形。	一、第一項規定關鍵基礎設施提供者之指定。關鍵基礎設施提供者之資通安全維護，乃現今國際針對資通安全保護所重視之議題，爰參考歐盟二〇一六年「網路與資訊系統安全指令」（The Directive on security of network and information systems）第五條關於關鍵服務營運商之清單、第十四條關於關鍵服務營運商用以提供關鍵服務之網路與資訊系統，如有影響其安全之事件，關鍵服務營運商須採取適當措施及最小化事件之影響，以確保服務之持續性、美國 6 USC§132 指定關鍵基礎設施保護計畫（Designation of critical infrastructure protection program）及第一三六三六號行政命令有關改善關鍵基礎設施網路安全（Executive Order 13636）、日本網路安全基本法第六條重要社會

維護計畫實施有缺失或待改善者，應提出改善報告，送交中央目的事業主管機關或直轄市、縣（市）政府。 第二項至第五項之資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，由中央目的事業主管機關擬訂，報請行政院核定之。		基礎業者之職責、韓國情報通信基礎保護法第八條中央行政機關長官有權指定主要資訊通信基礎設施及同法第五條主要資訊通信基礎設施保護措施之制定等立法例，將關鍵基礎設施提供者納入本法之適用範圍。 二、因關鍵基礎設施涉及國家安全、社會公共利益、國民生活及經濟活動，爰於第二項規定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，並訂定、修正及實施資通安全維護計畫，以確保其資通安全。 三、為使中央目的事業主管機關及直轄市、縣（市）政府掌握所管關鍵基礎設施提供者之資通安全維護計畫實施狀況，爰於第三項規定關鍵基礎設施提供者應向中央目的事業主管機關或直轄市、縣（市）政府提出資通安全維護計畫實

		施情形，以利中央目的事業主管機關或直轄市、縣（市）政府監督，並適時提供相關建議或協助。 四、為確保資通安全維護計畫之落實，於第四項規定中央目的事業主管機關或直轄市、縣（市）政府應稽核所管關鍵基礎設施提供者之資通安全維護計畫實施情形。稽核時，宜考量受稽核者歷來接受行政院、中央目的事業主管機關或直轄市、縣（市）政府稽核之頻率與稽核結果等因素，決定最適之受稽核者名單與頻率。 五、第五項規定關鍵基礎設施提供者之資通安全維護計畫實施情形有缺失或待改善者，應提出改善報告，送交中央目的事業主管機關或直轄市、縣（市）政府，以確保資通安全維護計畫之落實。 六、考量資通安全維護計畫必要事項、實施情形之

		提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，其內容宜有一致性，以利關鍵基礎設施提供者適用與遵循，爰於第六項規定，由中央目的事業主管機關擬訂，並報請行政院核定之。 七、中央目的事業主管機關宜訂定非公務機關資通安全維護計畫之範本，以供非公務機關參考；行政院並得提供必要之協助。 **本報告說明：** 為明確規範政府機關（構）資通安全責任等級分級作業流程，建議宜由中央目的事業主管機關、直轄市或縣（市）政府擬訂一套完善之資通安全維護計畫有關之必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，再報請行政院核定。爰刪除第十五條第四項至第六項，統一規定於第六條第三項。

第十六條　關鍵基礎設施提供者以外之非公務機關，應符合其所屬資通安全責任等級之要求，並考量其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。 中央目的事業主管機關或直轄市、縣（市）政府得要求所管前項非公務機關，提出資通安全維護計畫實施情形。 中央目的事業主管機關或直轄市、縣（市）政府得稽核所管第一項非公務機關之資通安全維護計畫實施情形，發現有缺失或待改善者，應限期要求受稽核之非公務機關提出改善報告。 前三項之資通安全維護計畫必要事項、實施情形之提	第十六條　關鍵基礎設施提供者以外之非公務機關，應符合其所屬資通安全責任等級之要求，並考量其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。 中央目的事業主管機關或直轄市、縣（市）政府得要求所管前項非公務機關，提出資通安全維護計畫實施情形。	**行政院說明：** 一、考量關鍵基礎設施提供者以外之非公務機關亦應負相當之資通安全責任，仍應訂定安全維護計畫並提出計畫實施情形，爰參考日本網路安全基本法第三條賦予重要社會基礎業者配合政府資通安全政策之協力義務之規定，於第一項明定該等非公務機關應符合其所屬資通安全責任等級之要求，並修訂及實施資通安全維護計畫。 二、鑒於資通安全維護事項與事業之經營管理關係密切，對於非公務機關資通安全維護之指導、監督、管理及稽核，宜由各非公務機關之中央目的事業主管機關或直轄市、縣（市）政府執行，爰為第二項及第三項規定。 三、考量資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之

出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，由中央目的事業主管機關擬訂，報請行政院核定之。		提出及其他應遵行事項之辦法，其內容宜有一致性，以利第一項之非公務機關適用與遵循，爰於第四項規定，由中央目的事業主管機關擬訂，並報請行政院核定之。 四、中央目的事業主管機關宜訂定非公務機關資通安全維護計畫之範本，以供非公務機關參考；行政院並得提供必要之協助。 **本報告說明：** 為明確規範政府機關（構）資通安全責任等級分級作業流程，建議宜由中央目的事業主管機關、直轄市或縣（市）政府擬訂一套完善之資通安全維護計畫有關之必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，再報請行政院核定。爰刪除第十六條第三、四項，統一規定於第六條第三項。
第十七條　非公務機關為因應資通安全	第十七條　非公務機關為因應資通安全	**行政院說明：** 一、為使中央目的事業主管

事件，應訂定通報及應變機制。 非公務機關於知悉資通安全事件時，應向中央目的事業主管機關或直轄市、縣（市）政府通報。 非公務機關應向中央目的事業主管機關或直轄市、縣（市）政府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，並應送交行政院。 前三項通報及應變機制之必要事項、通報內容、報告之提出及其他應遵行事項之辦法，由行政院定之。 知悉重大資通安全事件時，行政院、中央目的事業主管機關或直轄市、縣（市）政府，於適當時機得公告與事件相關之必要內容及因應措施，並得提供相	事件，應訂定通報及應變機制。 非公務機關於知悉資通安全事件時，應向中央目的事業主管機關或直轄市、縣（市）政府通報。 非公務機關應向中央目的事業主管機關或直轄市、縣（市）政府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，並應送交行政院。 前三項通報及應變機制之必要事項、通報內容、報告之提出及其他應遵行事項之辦法，由行政院定之。 知悉重大資通安全事件時，行政院、中央目的事業主管機關或直轄市、縣（市）政府，於一個月內得公告與事件相關之必要內容及因應措施，並得提供相	機關、直轄市、縣（市）政府及行政院即時掌握非公務機關之資通安全事件，監督及協助該等非公務機關進行緊急應變處置，並在最短時間內回復業務正常運作，爰參考歐盟二〇一六年「網路與資訊系統安全指令」第十四條事件通知、日本網路安全基本法第十四條促進重要社會基礎業者確保網路資訊安全、韓國情報通信基礎保護法第十六條於金融、通信等領域別之情報通信基礎設施業者得依法成立及運作情報共有、分析中心，作為有侵害事故時之即時警報與分析體系等規定，為第一項至第三項規定。有關資通安全事件之內涵，同第十三條說明一；重大資通安全事件之認定，將於施行細則中規範。 二、第四項明定第一項至第三項通報及應變機制之必要事項、通報內容、

關協助。	關協助。	報告之提出及其他應遵行事項之辦法，由行政院定之，以利非公務機關依循。 三、考量重大資通安全事件可能影響多數人民之生命、身體或財產安全，宜由行政院、中央目的事業主管機關或直轄市、縣（市）政府於知悉後，分別或共同公告必要之內容（例如發生原因、影響程度及目前控制之情形等）及因應措施，並提供相關協助，以利防範、避免損害之擴大，爰為第五項規定。 **本報告說明：** 考量重大資通安全事件可能影響多數人民之生命、身體或財產安全，然第十七條第五項僅規範於「適當時機」得公告與事件相關之必要內容及因應措施，並無明確之時間，未明文規範恐形成認知上之不同，為求明確與嚴謹，宜盡量避免解釋上可能產生歧異之用字或句法；為使文義明確，須在一定時間內將問題癥結查明，且因考

		量資訊技術發展快速，為爭取時效，爰建議宜訂為一個月內公告，使各單位對類此事件有所警惕與防範。
第十八條　中央目的事業主管機關或直轄市、縣（市）政府因稽核資通安全維護情形發現重大缺失，或遇重大資通安全事件，而認有必要時，得派員攜帶執行職務證明文件，進入非公務機關場所檢查，並得命相關人員為必要之說明、配合措施或提供相關證明資料。 對於前項之檢查，非公務機關及其相關人員無正當理由不得規避、妨礙或拒絕。 參與檢查之人員，對於因檢查而知悉之他人應秘密之資訊，負保密義務。	第十八條　中央目的事業主管機關或直轄市、縣（市）政府因稽核資通安全維護情形發現重大缺失，或遇重大資通安全事件，而認有必要時，得派員率同法律及其他專業人員，攜帶檢查證及執行職務證明文件，進入非公務機關場所檢查，並得命相關人員為必要之說明、配合措施或提供相關證明資料。 對於前項之檢查，非公務機關及其相關人員無正當理由不得規避、妨礙或拒絕。 參與檢查之人員，對於因檢查而知悉之他人應秘密之資訊，負保密義務。	**行政院說明：** 一、為落實非公務機關資通安全之維護，應賦予監督機關有命令、檢查及處分權，爰參考日本網路安全基本法第十五條第二項政府為促進民間業者採取自發性之措施得採取必要措施，與同法第十七條政府為取締犯罪及防止傷害之擴大得採取必要措施之規定，為第一項及第二項規定，以強化中央目的事業主管機關與直轄市、縣（市）政府之權責。 二、為保護個人資料及其他他人應秘密之資訊，爰於第三項明定因檢查而知悉他人應秘密之資訊者，應負保密義務。 **本報告說明：** 一、有論者主張稽核資通安全維護情形發現有必要時，得派員攜帶執行職務證明文件，進入非公

		務機關場所檢查，此檢查制度形同於刑事訴訟法中搜索扣押，有違憲之虞。另有論者主張此等稽核或派員檢查手段，對於民間業者之營業秘密保障有所侵害。對民間單位加以稽核或派員檢查，究竟在維護資通安全此等目的下，是否合乎於憲法比例原則之要求有所疑慮。然必須知道的是，對於此等資訊通訊產業而言，其資通安全之設計，例如程式碼設計或硬體配置等，與業者之智慧財產權及營業方式具有高度相關，對於業者之財產權、隱私權以及營業自由等權利具有密切之關連，而行政單位要求其提出相關資訊時，對於業者之權利侵害不可謂之不巨大，且必須考慮資安的專業性以及其中涉及業者的營業秘密與相關智慧財產權等，其稽核的方法、手段、頻率乃至於派員檢查之相

		關程序究竟應如何規定，亦為政府所必要多加考量者。 二、持平而論，現行法規中已有許多關於行政檢查之規定，本草案第十八條之規定並非首例，惟因本草案牽涉資訊系統部分至為重要且敏感，對於非公務機關之資訊隱私、營業秘密及法遵成本亦應妥善加以考量。其檢查人員之資格應加以明確界定，因於草案第五條規定行政院得委任或委託其他公務機關、法人或團體，辦理資通安全整體防護、國際交流合作及其他資通安全相關事務；第八條規定公務機關或非公務機關可委外辦理資通系統之建置、維運或資通服務之提供，顯見辦理資通安全相關事務者並非全為公職人員，受委任或委託之非公職人員即使攜帶執行職務證明文件，進入非公務機關場所檢查，其身分及公

		信力仍值得商榷；故檢查人員之身分及資格宜詳加規範與斟酌，畢竟此與民眾之財產權、隱私權及營業秘密等權利影響甚鉅，應審慎為之；執行時應有具法律及其他專業之人員陪同，以維護基本人權及避免侵權。
第四章　罰則	（無修正意見）	章名。
	第○○條　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。	一、本條係新增。如獲採納條次列為第十九條，原第十九條以下條文之條號應配合調整。 二、第十四條係將公務機關所屬人員對於資通安全管理之獎勵、懲戒與懲處，列於第二章之公務機關資通安全管理，然於第四章罰則之第十九條至第二十一條皆為非公務機關違反資通安全之處罰，此易造成誤解為罰則僅針對非公務機關而不處罰公務機關所屬人員，故將第十四條第二項，移列另立新條文，以示明確與一致。

第十九條　非公務機關有下列情形之一者，由中央目的事業主管機關或直轄市、縣（市）政府令限期改正；屆期未改正者，按次處新臺幣十萬元以上一百萬元以下罰鍰： 一、未依第十五條第二項或第十六條第一項規定，訂定、修正或實施資通安全維護計畫，或違反第十五條第六項或第十六條第四項所定辦法中有關資通安全維護計畫必要事項之規定。 二、未依第十五條第三項或第十六條第二項規定，向中央目的事業主管機關或直轄市、縣（市）政府提出資通安全維護計畫之實施情形，或違反第十五條第六項或第十六條第	第十九條　非公務機關有下列情形之一者，由中央目的事業主管機關或直轄市、縣（市）政府令限期改正；屆期未改正者，按次處新臺幣十萬元以上一百萬元以下罰鍰： 一、違反第六條第二項所定辦法中有關資通安全維護計畫必要事項之規定，或未依第十五條第二項或第十六條第一項規定，訂定、修正或實施資通安全維護計畫。 二、違反第六條第二項所定辦法中有關資通安全維護計畫實施情形提出之規定，或未依第十五條第三項或第十六條第二項規定，向中央目的事業主管機關或直轄市、縣（市）政府提出資通安	**行政院說明：** 參考歐盟二〇一六年「網路與資訊系統安全指令」第二十一條要求會員國必須針對違反相關國家法規之行為，制定有效罰則之意旨，並考量違反本法所定行政法上義務應受責難程度及其所生影響，針對非公務機關未依本法規定訂定、修正、實施資通安全維護計畫、提出資通安全維護計畫之實施情形、改善報告送交中央目的事業主管機關或直轄市、縣（市）政府、訂定資通安全事件之通報及應變機制、向中央目的事業主管機關、直轄市、縣（市）政府或行政院提出資通安全事件之調查、處理及改善報告，或違反資通安全事件通報內容之規定等情形，明定所課予之行政裁罰。 **本報告說明：** 為配合刪除第十五條第六項及第十六條第四項，爰修正第一款至第三款文字中之條次規定。

四項所定辦法中有關資通安全維護計畫實施情形提出之規定。 三、未依第六條第三項、第十五條第五項或第十六條第三項規定，提出改善報告送交行政院、中央目的事業主管機關或直轄市、縣（市）政府，或違反第十五條第六項或第十六條第四項所定辦法中有關改善報告提出之規定。 四、未依第十七條第一項規定，訂定資通安全事件之通報及應變機制，或違反第十七條第四項所定辦法中有關通報及應變機制必要事項之規定。 五、未依第十七條第三項規定，向中央目的事業主管機關、直轄市、縣（	全維護計畫之實施情形。 三、違反第六條第二項所定辦法中有關改善報告提出之規定，或未依第六條第三項規定，提出改善報告送交行政院、中央目的事業主管機關或直轄市、縣（市）政府。 四、未依第十七條第一項規定，訂定資通安全事件之通報及應變機制，或違反第十七條第四項所定辦法中有關通報及應變機制必要事項之規定。 五、未依第十七條第三項規定，向中央目的事業主管機關、直轄市、縣（市）政府或行政院提出資通安全事件之調查、處理及改善報告，或違反第十七條第四項	

市)政府或行政院提出資通安全事件之調查、處理及改善報告,或違反第十七條第四項所定辦法中有關報告提出之規定。 六、違反第十七條第四項所定辦法中有關通報內容之規定。	所定辦法中有關報告提出之規定。 六、違反第十七條第四項所定辦法中有關通報內容之規定。	
第二十條　非公務機關未依第十七條第二項規定,通報資通安全事件,由中央目的事業主管機關或直轄市、縣(市)政府處新臺幣十萬元以上一百萬元以下罰鍰,並令限期改正;屆期未改正者,按次處罰之。	(無修正意見)	參考歐盟二〇一六年「網路與資訊系統安全指令」第二十一條要求會員國必須針對違反相關國家法規之行為,制定有效罰則之意旨,並考量違反本法所定行政法上義務應受責難程度及其所生影響,針對非公務機關未依第十七條第二項規定,通報資通安全事件之情形,明定所課予之行政裁罰。
第二十一條　非公務機關違反第十八條第二項規定者,由中央目的事業主管機關或直轄市、縣(市)政府處新臺幣十萬元以上一百萬元以下罰鍰。	(無修正意見)	參考歐盟二〇一六年「網路與資訊系統安全指令」第二十一條要求會員國必須針對違反相關國家法規之行為,制定有效罰則之意旨,並考量違反本法所定行政法上義務應受責難程度及其所生影響,針對非公務機關無正當

		理由妨礙、規避或拒絕行政檢查之情形，明定所課予之行政裁罰。
第五章　附則	（無修正意見）	章名。
第二十二條　本法施行細則，由行政院定之。	（無修正意見）	本法施行細則之訂定機關。
第二十三條　本法施行日期，由行政院定之。	（無修正意見）	本法施行日期，考量配套子法作業時程，並為周延法制，以落實本法規定之執行，爰授權由行政院定之。

參考文獻

一、政府出版品、圖書、論文

1.立法院第 9 屆第 3 會期第 13 次會議議案關係文書，院總第 1570 號　政府提案第 15966 號。

2.立法院第 9 屆第 1 會期第 10 次會議議案關係文書，《行政院函送本院委員黃國昌等 11 人於第 9 屆第 1 會期第 4 次會議所提臨時提案之研處情形》，105 年 4 月 20 日。

3.行政院，《國家關鍵基礎設施安全防護指導綱要》，103 年 12 月 29 日。

4.行政院，《行政院法案及性別影響評估檢視表》，105 年 12 月 2 日。

5.行政院國家資通安全會報，《國家資通安全通報應變作業綱要》，105 年 8 月 1 日。

6.張裕榮，《國家資通安全科技中心設置條例草案評估報告》，立法院法制局法案評估報告，編號 970，103 年 9 月。

7.經濟部智慧財產局，《營業秘密保護實務教戰手冊》，102 年 12 月。

二、期刊、報紙

1.《莫因資訊揭露 衝擊企業營業秘密》，工商時報社論－火線焦點，106 年 5 月 31 日。

三、網路資源

1.方鴻春，「我國關鍵基礎建設安全防護」，《清流月刊》，98 年 2 月號，
http://www.mjib.gov.tw/FileUploads/eBooks/a7d057a843434ac1a4a44eaf53f4bd2c/Book_file/4843f93495f246b1854bd1054e4a7211.pdf，參閱日期 106 年 5 月 4 日。

2.立法院國會圖書館法律系統，「國家資通安全科技中心設置條例」廢止理由
http://lis.ly.gov.tw/lglawc/lawsingle?000742D7BB780000000000000000005000000000B000000^02822105050300^00123001001，參閱日期 106 年 5 月 31 日。

3.司法院大法官解釋釋字第 603 號，94 年 9 月 28 日，
http://www.judicial.gov.tw/constitutionalcourt/p03_01.asp?expno=603，參閱日期 106 年 5 月 25 日。

4.科技產業資訊室（iKnow ）張小玫、杜君妮，《世界經濟論壇(WEF)發佈「全球風險報告」》，106 年 2 月 8 日，
http://iknow.stpi.narl.org.tw/Post/Read.aspx?PostID=13172，參閱日期 106 年 5 月 12 日。

5.黃俊能，《國家關鍵基礎設施防護之推動與策略－脆弱度評估與風險思維》，ithomew－臺灣資安大會－關鍵基礎建設安全論壇，
https://cyber.ithome.com.tw/2017/forum5，參閱日期 106 年 5 月 12 日。

6.黃彥棻，「尋找臺灣資安新動能系列報導（一）：2017 年政府資安

預算編列 25 億元，歷年最高」,《資安周報第 56 期》，106 年 1 月 4 日，http://www.ithome.com.tw/news/110923，參閱日期 106 年 5 月 10 日。

7.達信台灣（MARSH）,《觀察 2017 年全球風險報告》，106 年 1 月 23 日，http://asia.marsh.com/taiwan/%E8%A7%80%E5%AF%9F%E8%88%87%E8%A7%A3%E6%B1%BA%E6%96%B9%E6%A1%88/ThoughtLeadership/ID/47172/2017.aspx，參閱日期 106 年 5 月 15 日。

8.維基百科,《商業秘密》，最後修訂於 105 年 1 月 29 日，https://zh.wikipedia.org/wiki/%E5%95%86%E4%B8%9A%E7%A7%98%E5%AF%86，參閱日期 106 年 5 月 18 日。

9.盧映潔、林伯樺,《盧映潔觀點：「資通安全管理法草案」之修正建議》，風傳媒，106 年 5 月 15 日，http://www.storm.mg/article/264648，參閱日期 106 年 5 月 15 日。

10.VINCENT CHEN,《資訊發展與安全管理立法之觀察與建議》,105 年 9 月 6 日，https://rocket.cafe/talks/79059，參閱日期 106 年 5 月 10 日。

11. https://www.congress.gov/bill/113th-congress/senate-bill/2521/text?overview=closed，參閱日期 106 年 6 月 15 日。

附錄

一：「資通安全管理法草案」評估報告（初稿）座談會紀錄及參採情形

時間：中華民國 106 年 7 月 6 日（星期四）上午 10 時

地點：立法院法制局 305 會議室

主席 ：劉厚連 組長　　記錄：陳淑敏、曾耀民

出席人員：

一、學者專家:

大同大學資訊經營學系　　教授　陳志誠

二、機關代表:

行政院

資通安全處　　副處長　徐嘉臨

分析師　賴世榮

副研究員 楊　祁

三、本局同仁：

助理研究員 方華香

發言要點：

陳教授志誠：

一、本人學資訊，是資訊人員，當過公務員及老師，目前任教於大同大學及德國斯圖加大學。信用卡刷卡簡訊回復是本人於 15 年

前做出來的，警政署 110 報案系統由本人規劃並完成，還有防災資料庫也是本人做的，我們的第一批網軍刑事警察局偵九隊也是本人所培養出來。資通安全管理法草案的訂定，本人以為要列入三個觀點：其一，技術演進觀點，因為資訊技術進步很快；其二，資訊社會生態，資訊社會是虛擬的，與實體不一樣；其三，網際網路的特點是沒有主管，要自主管理，所以資安沒有任何主管。至於本法是否要訂主管機關?本人認為資通安全要自主管理，不可能有主管機關，例如國人頭疼的食安問題也是要自主管理才能做好。

二、資通安全沒有絕對的安全，只有降低風險至可以正常營運，所以資通安全不可能由行政院管理所有其他單位的資通安全，這是不可能做得到的。關於關鍵基礎設施的資通安全，軟體與硬體其實是合在一起，更重要的是要自主管理，ISO 認證非常重要，要將資安責任推到各單位，落實各機關自主管理，自己負責，而非由行政院下令全國遵守。

三、本草案目的在使資安管理更好，或處罰不遵守資安規定，或資安單位法制化，本人看不出來。ISO 認證很重要，各單位要自主管理，成立資安管理委員會，負責人為副首長，實務運作上由資訊技術人員擔任。資安情勢變化很快，年年不同，例如今年的主軸為 AI(Artificial Intelligence, 人工智慧)，明年如何沒有人知道，但明年起機器人可以相互對話，已不是天方夜譚。由於資安情勢變化非常快速，資通安全情勢報告最多一年要提出，甚至是適當時機就要提出來，資安事件發生應該要立即通報。

四、防制大陸網軍很重要，我參加台灣駭客年會兩位上座者皆是台

中一中學生，年紀很輕，大陸培養的網軍幾乎全是高中生，台灣成為其演練沙場，大陸在台灣布建殭屍網路一直存在根本沒有撤，迄今大陸在台灣仍維持有百萬殭屍網路。資安管理宜重實質效益，要自主管理，提升資安防護能力。例如金管會應要求所有上市櫃公司做好資通安全。台灣的態度太保守，對新技術的抵制使經濟無法發展，例如 Uber、Airbnb 均被排斥在外。十多年前我到司法官訓練所開會及上課了很久，才使司法官能接受數位相片做為證據。我們應促使現有的舊法令調整迎接新技術，不宜墨守舊法令去抗拒新技術之時代浪潮，可行方法譬如事先給予業者一年時間做調適與準備。

參採情形：

一、針對上述發言一之意見：有關「主管機關」部分，同行政院發言一之參採情形。

二、針對上述發言二之意見：尚難成為具體可行條文，納入修正草案相關條文，爰照錄供參。

三、針對上述發言三之意見：有關「資通安全情勢報告」部分，同行政院發言五之參採情形。

四、針對上述發言四之意見：尚難成為具體可行條文，納入修正草案相關條文，爰照錄供參。

行政院：

一、有關建議增訂本法之主管機關（新增第 2 條），本院回應說明如下：本法草案由本院擬具，本院為本法之主管機關當無疑義，

考量本草案各條文規範事項之權責機關非僅限本院及地方政府，尚包含各中央目的事業主管機關、總統府、其他四院等，且現行法律亦有未定明主管機關者(例如行政程序法、行政罰法、訴願法、環境基本法、科學技術基本法等)，故未於本法明定主管機關，本草案並已明定各機關權責，建議維持原條文。此外，依本院處務規程第 17 條之 1 規定，資通安全處掌理國家資通安全之政策研議、法案審查、計畫核議、業務推動、督導及管考等事宜，其中包括國家關鍵資訊基礎設施安全管理機制。另依本院國土安全辦公室訂定之「國家關鍵基礎設施安全防護指導綱要」，已將我國關鍵基礎設施區分為能源、水資源、通訊傳播、交通、金融與銀行、緊急救援與醫院、中央與地方政府機關、科技園區與工業區等八個領域，並由該辦公室會同資通安全處就我國關鍵基礎設施中涉及資通安全部分定為關鍵資訊基礎設施，每年定期擇定不同領域之設施，辦理資通安全防護演練，並無業務重疊之處。

二、有關建議宜將關鍵基礎設施加以明確定義（草案第 2 條第 1 項第 6 款），本院回應說明如下：本草案所定義之關鍵基礎設施係沿用本院訂定之「國家關鍵基礎設施安全防護指導綱要」，本院國土安全辦公室已將我國關鍵基礎設施區分為能源、水資源、通訊傳播、交通、金融與銀行、緊急救援與醫院、中央與地方政府機關、科技園區與工業區等八個領域，並由該辦公室會同資通安全處就我國關鍵基礎設施中涉及資通安全部分定為關鍵資訊基礎設施。此外，前揭指導綱要原則每 2 年將定期檢討調整，關鍵基礎設施範圍亦配合國家發展情勢修正調整，未來關鍵基礎設施範圍可能不限於前述八個領域，為保留規範彈性，

建議維持原條文。

三、有關建議刪除草案第 2 條第 1 項第 7 款中之「依第十五條第一項規定」文字，本院對於上開建議修正之文字無意見。

四、有關建議增列重大資安事件之定義(草案第 2 條第 1 項第 8 款)，本院回應說明如下：以施行細則補充母法用詞規定，實務上已有類似之立法體例(例如勞動檢查法施行細則第 31 條、消費者保護法施行細則第 40 條、政府採購法施行細則第 111 條等)。依現行資通安全通報應變之實務運作，目前規範之重大資安事件型態不僅限於建議條文所列情形，所謂重大資安事件係指現行「國家資通安全通報應變作業綱要」所稱第 3 級及第 4 級資安事件，其定義將明定於本草案授權訂定之相關子法中，建議維持原條文。

五、有關建議每 2 年公布國家資通安全情勢報告及資通安全發展方案（草案第 4 條），本院回應說明如下：為統籌並加速我國資通安全基礎建設，本院於 90 年 1 月成立資安會報，即每 4 年循序推動為期 4 年之國家資通安全建設方案 (計畫)，包括 90 至 93 年及 94 至 97 年「建立我國通資訊基礎設施安全機制計畫」(通稱第一期及第二期資安機制計畫)，98 至 101 年及 102 至 105 年「國家資通訊安全發展方案」(通稱第三期及第四期資安發展方案)。在政府與民間共同合作下，已逐步建立國家資通安全防護機制，依目前積極研擬之第五期資安發展方案，其內容均以四年期為政策規劃期程，另有關資通安全情勢報告，則須視整體情勢發展調整適當之發布時機，可每年或每 2 年發布，為保留一定彈性，建議維持原條文。

六、有關對委任及委託者之資格與責任宜訂定相關辦法（草案第 5 條），本院回應說明如下：除政策制定或核心業務等本質上不宜

委任或委託辦理之事務外，資通安全相關事務權限之委任或委託，可依行政程序法第 15 條或第 16 條規定辦理，本草案第 5 條已明定本院委任或委託之依據。此外，本院為善用民間資源，降低政府財政負擔，提升公共服務效率，亦訂有「行政院及所屬各機關推動業務委託民間辦理實施要點」規範各委外事務。有關建議訂定相關辦法規範委任或委託之事項（受委任或委託者之資格、條件、責任、監督及其他應遵行事項），考量上開事項於實務上似需視資安情勢發展之彈性調整，多係透過委託契約方式訂定，如訂定辦法規範恐失彈性，應無另定子法之必要，建議維持原條文。

七、有關建議非公務機關資通安全維護計畫實施情形之稽核宜由中央目的事業主管機關擬訂，報請行政院核定之（草案第 6 條、第 15 條、第 16 條及第 19 條），本院回應說明如下：依所建議條文內容，改由本院、中央目的事業主管機關、直轄市及縣（市）政府應稽核非公務機關之資通安全維護計畫實施情形，反將造成非公務機關、關鍵基礎設施提供者受稽核頻率過高之疑慮。按本草案條文規定，本院得稽核非公務機關之資通安全維護計畫實施情形，而中央目的事業主管機關或直轄市、縣（市）政府應稽核所管關鍵基礎設施提供者，或得稽核公營事業及政府捐助之財團法人，此設計係配合實務運作並保留彈性，以及考量本院自身整體執行量能。另為利本院監督非公務機關實施資通安全維護計畫實施情形，爰由本草案授權本院就稽核頻率、內容與方法及其他相關事項訂定子法。本院未來進行上開稽核時，將考量受稽核對象過往資通安全維護狀況，以及歷來接受本院、中央目的事業主管機關或直轄市、縣（市）政府稽核之

頻率、結果，決定最適之稽核名單，以避免產生重複稽核情形，建議維持原條文。

八、有關建議納入「年度評估報告」，以加強系統化資通安全風險管理（草案第 11 條），本院回應說明如下：按本院依本草案授權刻正研訂之「資通安全維護計畫實施情形稽核辦法」草案已規範資通安全維護計畫之事項，包括其實施情形之定期評估、稽核機制、缺失之消除或改正，其中稽核機制即指內稽及外稽(委由第三方稽核)，所提建議條文之年度評估報告應可含括於前述機制中，毋須另行規定，建議維持原條文。

九、有關建議將公務機關所屬人員之懲戒與懲處改列至罰則專章（草案第 14 條第 2 項改列為第 20 條），本院對於上開將公務機關所屬人員之懲戒或懲處規定改列至罰則專章之建議無意見。

十、有關重大資通安全事件之公告時間由適當時機改為 1 個月內（草案第 17 條第 5 項），本院回應說明如下：考量重大資安事件發生情形、涉及範圍、需公告之必要內容及因應措施各不相同，其公告之適當時機宜以個案認定，為保留實務運作彈性，爰不宜於法律中明定公告時間，建議維持原條文。

十一、有關進入非公務機關場所檢查之程序應更嚴謹與完備（草案第 18 條第 1 項），本院對於上開建議修正之文字無意見。

參採情形：

一、針對上述發言一之意見：所謂「主管機關」，乃指主管事務之機關；由於行政法規大部分涉及人民權利義務事項，且其內容每具強制性，爰有明定權責機關負責其事務之必要（「人事行政法制作業錦囊」，行政院人事行政總處編印，105 年 10 月，第 25

頁)。法規應明定主管機關，以明權責單位，向為我國作用法之立法通例，且法律規定之主管機關乃為整體、抽象之管轄權歸屬概念，並非法律規範之所有事項均應由主管機關負責執行(行政院法規委員會 92、93 年度諮詢會議有關法制事項之結論或共識，94 年 2 月 1 日)。復依中華民國憲法第 53 條規定：「行政院為國家最高行政機關」，由於中央行政機關均由行政院管轄，因此在中央層級法律中，多以「行政院」來代稱所有的中央行政機關，且於行政院 105 年 9 月 6 日舉辦之「資通安全管理法（草案）」政府機關座談會紀錄綜合討論一、出席人員主要關心議題之（六）、105 年 9 月 8 日舉辦之民間團體座談會紀錄綜合討論一、出席人員主要關心議題之（五）、105 年 9 月 13 日舉辦之學者專家座談會紀錄綜合討論一、出席人員主要關心議題之（二），及 105 年 9 月 20 日舉辦之學者專家第 2 場座談會紀錄綜合討論一、出席人員主要關心議題之（一），皆對主管機關權責事項相當關注，建議主管機關應予清楚定義並釐清資訊、資安主責單位，爰此，乃有建議增列主管機關之構想。然基於尊重行政院考量本草案各條文規範事項之權責機關非僅限行政院及地方政府，尚包括各中央目的事業主管機關、總統府及其他四院等之意見，同意參採並修正本報告。

二、針對上述發言二之意見：立法體例有（一）列舉規定：係為避免法規適用時發生疑義，故將所要規定要件、標準等具體之事物，以項、款逐一舉出，用以說明某一上位概念的意義或該列舉事物之總效果者稱之。(二) 例示規定：以例指或指示事物或種類之方式說明某一上位概念的意義。(三)例示兼概括規定(折衷規定)：按列舉(例示)事項屬於概括文句所表示之事項之一，

而概括文句卻不包括與列舉（例示）事項性質不相同之事項。行政院稱因考量「國家關鍵基礎設施安全防護指導綱要」原則每 2 年定期檢討調整，關鍵基礎設施範圍亦配合國家發展情勢修正調整，未來關鍵基礎設施範圍可能不限於前述 8 個領域，然若依照草案對於關鍵基礎設施之定義過於抽象且無具體之範圍，建議修正之文字係採例示兼概括規定，且敘明須經行政院公告，並非沒有彈性，況且目前之 8 個領域包含範圍實已相當廣泛。是以，仍維持原建議條文。

三、針對上述發言三之意見：對於本報告建議修正之文字無意見。

四、針對上述發言四之意見：基於法律之位階與明確性，應將與當事人重要權益且必須之要件直接於「資通安全管理法」明列規範，既可強化其位階性，且符合法律保留原則。若法條用語因其抽象性、一般性而不夠明確，致生解釋上的疑義，則為所謂「不確定法律概念」。草案中對於重大資安事件並未予以詳加規範，易造成法律適用之隨意性，且建議增列重大資安事件之定義，係引用「國家資通安全通報應變作業綱要」之資安事件影響等級之第 4 級及第 3 級中較為嚴重之事件。是以，仍維持原建議條文。

五、針對上述發言五之意見：行政院於 90 年 1 月成立資安會報，即每 4 年循序推動為期 4 年之國家資通安全建設方案（計畫），包括 90 至 93 年及 94 至 97 年通稱第一期及第二期資安機制計畫，98 至 101 年及 102 至 105 年通稱第三期及第四期資安發展方案，依目前積極研擬之第五期資安發展方案，其內容均以 4 年期為政策規劃期程。然當初之時空環境與現今大不相同，資訊情勢瞬息萬變，宜與時俱進配合調整政策規劃期程與公布資通

安全情勢報告之時間。是以，仍維持原建議條文。

六、針對上述發言六之意見：尊重行政院考量實務上需視資安情勢發展之彈性調整，多係透過委託契約方式訂定，倘訂定辦法規範恐失彈性，同意參採並修正本報告。

七、針對上述發言七之意見：草案第 15 條及第 16 條條文疑太過繁瑣且重複敘述，仍建議宜由中央目的事業主管機關、直轄市或縣（市）政府擬訂一套完善之資通安全維護計畫有關之必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，再報請行政院核定。並略為修改建議修正條文為中央目的事業主管機關或直轄市、縣（市）政府應稽核所管關鍵基礎設施提供者，行政院得稽核之。是以，仍維持原建議條文。

八、針對上述發言八之意見：同方助理研究員發言四之參採情形。

九、針對上述發言九之意見：對於本報告建議無意見。

十、針對上述發言十之意見：重大資通安全事件可能影響多數人民之生命、身體或財產安全，須在一定時間內將問題癥結查明，且因考量資訊技術發展快速，為爭取時效並使文義明確，爰建議宜訂為 1 個月內公告，方能使各單位對類此事件有所警惕與防範。復依 105 年 8 月 1 日修正之「國家資通安全通報應變作業綱要」資通安全通報演練及防範惡意電子郵件社交工程演練均規定於演練完成後 1 個月內送交報告。是以，仍維持原建議條文。

十一、針對上述發言十一之意見：對於本報告建議修正之文字無意見。

方助理研究員華香：

一、本報告建議條文第 2 條建議增訂行政院為主管機關一節，則本草案其他條文中之「行政院」似應配合修正為「中央主管機關」；又本報告初稿第 11 頁提及行政院國家資通安全會報組織架構圖及相關論述一節，如本草案主管機關定為行政院，則行政院國土安全辦公室與資安處就相關業務有否重疊，事屬行政院內部分工，與本草案內容無涉，似無須再論。

二、本報告參考行政院「國家關鍵基礎設施安全防護指導綱要」對關鍵基礎設施之定義，建議本草案第 2 條第 1 項第 6 款增列八類主部門一節，其與「實體或虛擬資產、系統或網路」中似宜有連結詞，例如：「關鍵基礎設施：指能源、…、高科技園區等『部門之』實體或虛擬資產、系統或網路，其功能…」，以使語意明確。

三、本報告建議增列第 5 條第 2 項：「前項『委任或委託者』之資格、條件…之辦法，由行政院定之。」一節，查同條第 1 項所稱之委任或委託者應為行政院，無須再由行政院訂辦法，是以，本報告建議增列第 5 條第 2 項所稱『委任或委託者』等語，似有誤寫，建請更正。

四、本報告建議於本草案第 11 條納入「年度評估報告」一節，查該條後段所稱「無上級機關者」，包含行政院以外四院及總統府，每年均需將其資通安全維護計畫實施情形及「年度評估報告」送交行政院，對本院課予每年應做「年度評估報告」之義務，在行政院版本草案以外，更增加本院負擔，是否妥適，建請審酌。

五、本報告建議將公務機關所屬人員之懲戒與懲處改列至罰則專章

一節，係認為「草案第 4 章…皆為非公務機關違反資通安全之處罰，此易造成誤解為罰則僅針對非公務機關『而不處罰公務機關』，故建議宜將草案中有關之罰則統一規定於專章內…」，惟縱將公務機關所屬人員之懲戒與懲處改列至罰則專章，仍未罰及公務機關，僅罰及公務員。相關論述，是否調整，建請審酌。

六、本報告建議條文第 18 條第 1 項規定：「…攜帶由『各主管機關』核發之檢查證…」，由於本報告建議增訂行政院為本法之主管機關，且本條項又規定有「中央目的事業主管機關」、「直轄市、縣（市）政府」，條文中所稱之「各主管機關」究何所指？建請釐清明定為妥，以利適用。

參採情形：

一、針對上述發言一之意見：同行政院發言一之參採情形。

二、針對上述發言二之意見：已參採修正。

三、針對上述發言三之意見：同行政院發言六之參採情形。

四、針對上述發言四之意見：考量「無上級機關者」係包括總統府、本院、司法院、考試院、監察院、直轄市政府、縣（市）政府、直轄市議會及縣（市）議會等，行政院收受其資通安全維護計畫實施情形僅予以備查，無實質之監督效果，並恐有違權力分立之疑，基此，有關提出年度評估報告僅限於公務機關，已參採修正。

五、針對上述發言五之意見：係漏列「所屬人員」等字，已參採修正。

六、針對上述發言六之意見：配合不增列主管機關，故將建議修正

第 18 條第 1 項之「由各主管機關核發之」予以刪除，已參採修正。

（散會：上午 11 時 12 分）

二：行政院法案及性別影響評估檢視表

「法案及性別影響評估檢視表」

【第一部分】：本部分由機關人員填寫　　103.8.15

填表日期：105 年 12 月 2 日

填表人姓名：賴世榮　　職稱：分析師

電話：02-33568207　　e-mail：sjlai@ey.gov.tw

身分：■ 業務單位人員　□ 法制單位人員　□ 其他，請說明：_____

填 表 說 明

一、行政院所屬各機關主管法律案報院審查，應依「行政院所屬各機關主管法案報院審查應注意事項」及「中央行政機關法制作業應注意事項」規定辦理。

二、除廢止案（及配合行政院組織改造整批處理、單純訂修之法律案）外，皆應依據本表進行「法案及性別影響評估」。

三、建議各單位於法案研擬初期，即徵詢性別平等專家學者或各部會性別平等專案小組的意見；法案研擬完成後，應併同本表送請民間性別平等專家學者進行程序參與（至少預留 1 週的填寫時間），參酌其意見修正法案內容，並填寫「玖、性別影響評估結果」後通知程序參與者。

壹、法案名稱	資通安全管理法草案		
貳、主管機關	行政院	主辦機關	行政院（資通安全處）

參、法案內容涉及領域：	勾選（可複選）
3-1 權力、決策、影響力領域	
3-2 就業、經濟、福利領域	
3-3 人口、婚姻、家庭領域	
3-4 教育、文化、媒體領域	
3-5 人身安全、司法領域	
3-6 健康、醫療、照顧領域	
3-7 環境、能源、科技領域	√
3-8 其他（勾選「其他」欄位者，請簡述法案涉及領域）	

肆、問題界定與訂修需求

項目		說明	備註
4-1 問題界定	4-1-1 問題描述	隨著科技的蓬勃發展，資通科技與應用已是國人生活中重要的一環，例如無線網路、行動裝置、雲端服務、智慧聯網等新興資訊通信科技之使用均日趨普及，不同機關、組織間亦高度倚賴資通科技與應用彼此溝通或提供服務等，無論公務機關、非公務	簡要說明所面臨問題之梗概。

1

		機關或者一般民眾，日常作業或生活中均與資通科技密不可分，但隨之而來的資安風險也大幅增加。惟我國目前並無跨領域且以資通安全風險管理為核心之專門法令，難以滿足目前資通安全管理之需求。	
	4-1-2 執行現況及問題之分析	我國公務機關目前已設有資安推動單位，並訂有相關行政規則，包括行政院及所屬各機關資訊安全管理要點、行政院及所屬各機關資訊安全管理規範、國家資通安全通報應變作業綱要等，也有部分法令針對私部門之個別領域訂有資安相關規定，惟各法令分由不同部會職掌，其規範對象、規範方式與目的等均有其各自之重點，尚未能考量資通跨領域應用與互通之特性，而為共通之管理規範。	1.業務推動執行時，遭遇問題之原因分析。 2.說明現行法規是否不足、須否配合現況或政策調整。
	4-1-3 相關之性別統計及性別分析	本法草案內容涉及公務機關與非公務機關之資通安全維護義務，所以主要規範對象均為組織。惟關於人才培訓部分，在未來政府推動人才培育時，將搭配鼓勵少數性別參與之措施，例如：規劃培訓活動時，考量不同性別之參訓需求，如提供妥適的哺集乳空間；培訓時間避免影響接送年幼子女上下學之時段；培訓地點為大眾運輸系統便利之處或提供交通接駁服務；宣傳培訓活動時，為擴大參與，避免刻板印象，應納入鼓勵多元性別和族群參加之文字或圖片。	1.透過櫃檯資料庫、圖書等各種途徑蒐集既有的性別統計，並作出性別分析，以說明該問題是否會對不同性別人口造成不同影響。 2.性別統計與性別分析應儘量顧及不同性別、性傾向及性別認同者之年齡、族群、地區等面向。
	4-1-4 須強化的性別統計及其方法	本法草案內容涉及公務機關與非公務機關之資通安全維護義務，所以主要規範對象均為組織，故與性別較無關聯。	如既有性別統計不足，請提出須強化之處及其建置方法。
4-2 訂修需求	4-2-1 解決問題可能方案	透過本法草案之規範，要求公務機關、非公務機關以風險管理為核心，開展其資安防護計畫，並進行資安事件通報，應可解決現狀之不足。	請詳列解決問題之可能方案及其評估（涉及性別平等議題者，併列之）。

4-2-2 訂修必要性	本法草案之推動可促使公務機關及非公務機關，投入資通安全資源，並決定維護計畫並進行資安事件之通報，亦可解決現有法令未能考量資通安全跨領域並彼此影響之問題，故有訂定必要。	請說明最終必須訂修法案以解決問題之理由；如有立委提案，以風險管理為核心開展其資通安全並請納入研析。
4-3 配套措施及相關機關協力事項	本法草案如經立法通過，行政院及各中央目的事業主管機關應配合研訂相關辦法，並監督下級機關或所管之非公務機關，並應依需求編列預算與人力。	配套措施諸如人力、經費需求或法制整備等；相關機關協力事項請予詳列。
伍、政策目標	有效規劃我國之資通安全管理政策，並落實於公、私部門，以建構一個安全之資通環境，進而確保國家安全、民眾福祉。	簡要說明政策取向。

陸、徵詢及協商程序

項　目	說　明	備　註
6-1 法案主要影響對象	公務機關（包含中央、地方機關（構）及行政法人）及非公務機關（包括關鍵基礎設施提供者、其他公營事業及由公務機關或公營事業捐助成立之財團法人，且其捐助財產合計超過該財團法人之基金總額達行政院所定一定比例者）。	請說明法案內容主要影響之機關（構）、團體或人員。
6-2 對外意見徵詢	1. 為廣徵各界意見，已於 105 年 9 月 6 日、8 日、13 日、20 日(2 場)、23 日及 11 月 15 日邀集民間團體及學者專家辦理 7 場草案說明會(參與人數共計 179 人，其中男性 141 人，女性 38 人，男女比例約為 3.71:1)。 2. 為持續徵詢外界意見，並自 9 月 22 日起將本法草案及相關討論議題公布於國發會公共政策網路參與平台。 3. 後續進行本法草案及相關子法意	1. 請說明對社會各界徵詢意見及與相關機關（構）、地方自治團體協商之人事時地。 2. 徵詢或協商時，應敘明其重要事項、有無爭議、相關條文、主要意見、參採與否及其理由（含國際參考案例），並請填列於附表；如有其他相關資料，亦請一併檢附。 3. 對社會各界徵詢意見，應落

	見徵詢時，亦將特別留意性別比例。	實性別參與。
6-3 與相關機關（構）及地方自治團體協商	1. 為廣徵相關機關（構）及地方自治團體意見，已於 105 年 9 月 6 日辦理草案說明會，了解執行面之可行性及相關考量。 2. 本法草案擬定過程中，透由法務部法制司、行政院法規會及本處組成工作小組，並就條文進行逐條審議，確認法制上之可行性。	

柒、成本效益分析及對人權之影響：

項　目	說　明	備　註
7-1 成本	1. 受規範之公務機關及非公務機關，均應訂定資通安全維護計畫及通報應變機制，並視自身情形與需求編列預算。 2. 各公務機關與非公務機關之情形各異，需投入之成本將因而有異。	
7-2 效益	1. 建構國家資通安全環境。 2. 確保國家安全及民眾福祉。 3. 降低公務機關與非公務機關之財務及非財務損失。根據媒體 iThome 報導，80.1%的臺灣企業在去年曾經歷過 1 次以上的資安事件，臺灣企業因資安事件所受的財務損失，有 11%的企業評估損失金額在 50 萬元以下，5.9%企業自認損失超過百萬元；但以上尚未能評估未被通報之資安事件黑數，也未能評估資安事件對企業或民眾所	1.關於成本及效益，指政府及社會為推動及落實法案必須付出之代價及可能得到之效益。 2.得量化者應有明確數字，難以量化者亦應有詳細說明。

		造成的非財務損失；如能有更健全之資安管理，將能降低上述財務與非財務損失。	
7-3 對人權之影響	7-3-1 憲法有關人民權利之規定	本法草案符合憲法有關人民權利之相關規定。	請檢視法案是否符合憲法有關人民權利之規定及司法院解釋。
	7-3-2 公民與政治權利國際公約	本法草案符合公約規定及聯合國人權事務委員會之一般性意見。	依公民與政治權利國際公約及經濟社會文化權利國際公約施行法，請檢視法案是否符合公約規定及聯合國人權事務委員會之一般性意見，以積極促進各項人權之實現。
	7-3-3 經濟社會文化權利國際公約	本法草案符合公約規定及聯合國經濟社會文化權利委員會之一般性意見。	依公民與政治權利國際公約及經濟社會文化權利國際公約施行法，請檢視法案是否符合公約規定及聯合國經濟社會文化權利委員會之一般性意見，以積極促進各項人權之實現。

捌、性別議題相關性

8-1 規範對象：

（1）若 8-1 任一指標評定「是」者，應繼續填列項目「捌、8-2 及 8-3」及「第二部分一性別影響評估程序參與」；如 8-1 皆評定為「否」者，則免填「捌、8-2 及 8-3」，逕填寫「第二部分一性別影響評估程序參與」，惟若經程序參與後， 11-5「法案與性別議題關聯之程度」評定為「有關」者，則需修正「捌、8-1 至 8-3」，並補填列「玖、性別影響評估結果」。

（2）本項不論評定結果為「是」或「否」，皆需填寫評定原因。

項　目	評定結果(請勾選) 是	否	評定原因	備　註
8-1-1 訂修內容以特定性別、性傾向或性別認同者為規範對象		V	本法草案內容並無以特定性別、性傾向或性別認同者為規範對象。	如規範對象以男性或女性為主，或以同性戀、異性戀或雙性戀為主，或個人自認屬於男性或女性者，請評定為「是」。
8-1-2 訂修內容未區別對象，但執行方式將因性別、性傾向或性別認同不同		V	本法草案之對象及執行方式均不因性別、性傾向或性別認同不同而有差異。	規範對象雖無區別，但因性別、性傾向或性別認同之本質差異，而有不同執行方式者，請評定為「是」。

	而有差異		
8-1-3 訂修內容所規範對象及執行方式無差異，但對於不同性別、性傾向或性別認同者將產生不同結果	V	本法草案內容所規範對象及執行方式無差異，且對於不同性別、性傾向或性別認同者不會產生不同結果。	規範對象及執行方式雖無差異，惟其結果乃因性別、性傾向或性別認同而有不同者，請評定為「是」。

8-2 性別目標

項　目	說　明	備　註
8-2-1 採取積極作為，去除不必要差別待遇，或促進實質平等	（免填）	基於憲法平等權之規定，採行一定方式去除現行法規及其執行所造成之差別待遇，或提供較為弱勢之一方必要之協助，以促進其實質地位之平等。（本項及 8-2-2 不得全部填列無關）
8-2-2 營造平等環境，預防及消除性別歧視	（免填）	消除或打破性別刻板印象與性別隔離，以消弭因社會文化面向所形成之差異，或提供不同性別、性傾向或性別認同者平等機會獲取社會資源，提升其參與社會及公共事務之機會。（本項及 8-2-1 不得全部填列無關）

8-3 性別效益

項　目	說　明	備　註
8-3-1 對於消弭性別歧視、促進性別平等有積極、正面綜效	（免填）	請詳加說明性別效益何在，本項不得填列無關。
8-3-2 符合憲法、國際規範(包括消除對婦女一切形式歧視公約CEDAW)、性別平等政策綱領等要求	（免填）	依消除對婦女一切形式歧視公約施行法，請檢視法案是否符合公約(CEDAW)規定及其一般性建議，並請再查核法案內容之合宜性，本項不得填列無關。

玖、性別影響評估結果：請填表人依據性別平等專家學者意見之檢視意見提出綜合說明，包括對「第二部分、性別影響評估程序參與」主要意見參採情形、採納意見之法案調整情形、無法採納意見之理由或替代規劃等；經「第二部分－性別影響評估程序參與」後，11-5「法案與性別議題關聯之程度」評定為「無關」者，9-1至9-3免填。

9-1 評估結果之綜合說明	

9-2 參採情形	9-2-1 說明採納意見後之 法案調整	
	9-2-2 說明未參採之理由 或替代規劃	

9-3 通知程序參與之專家學者本法案的評估結果（請填寫日期及勾選通知方式，請勿空白）：

已於____年____月____日將「評估結果」以下列方式通知程序參與者審閱

□傳真　□e-mail　□郵寄　□其他_____

拾、法制單位復核（此欄空白未填寫者，將以不符形式審查逕予退件。）

10-1 法案內容：　□提經法規會討論通過　☑已會法制單位表示意見

10-2 徵詢及協商程序：　☑已徵詢及協商法案主要影響對象

☑已適當說明與回應徵詢及協商對象所提之主要意見

10-3 對人權之影響：　☑已由法規會具人權專長委員、曾受人權教育訓練之參事、其他高階人員或委請之人權學者專家檢視

10-4 訂修程序：　☑本檢視表已完整填列

復核人姓名及職稱：張嵐玲 諮議

【第二部分－性別影響評估程序參與】：本部分由性別平等專家學者填寫

拾壹、性別影響評估程序參與：若採用書面意見的方式，至少應徵詢 1 位以上性別平等專家學者意見，並填寫參與者的姓名、職稱及服務單位；專家學者資料可至台灣婦女館網站參閱（http://www.taiwanwomencenter.org.tw/）。

（一）基本資料		
11-1 程序參與期程或時間	105 年 11 月 29 日至 105 年 12 月 11 日	
11-2 參與者姓名、職稱、服務單位及其專長領域	姓名： 職稱： 服務單位： 專長領域：	
11-3 參與方式	□法案研商會議 □性別平等專案小組 ■書面意見	
11-4 業務單位所提供之資料	相關性別統計資料	法案內容
	□有 □很完整 □可更完整 □現有資料不足須設法 補足 ■無 ■應可設法找尋 □現狀與未來皆有困難	□有， 且具性別觀點 ■有， 但不具性別觀點 □無
11-5 法案與性別議題關聯之程度	□有關 ■無關 （若性別平等專家學者認為第一部分「捌、8-1 規範對象」8-1-1 至 8-1-3 任一指標應評定為「是」者，則勾選「有關」；若 8-1-1 至 8-1-3 均可評定「否」者，則勾選「無關」）。	
（二）主要意見：就前述各項之合宜性提出檢視意見，並提供綜合意見		
11-6 性別統計及性別分析之合宜性	如綜合檢視意見	
11-7 正當程序中性別參與之合宜性	如綜合檢視意見	
11-8 性別目標之合宜性	無	
11-9 性別效益說明之合宜性	無	

8

11-10 綜合性檢視意見	1. 法案內容涉及領域 建議亦勾選 3-7 環境、能源、科技領域 2. 6-2 對外意見徵詢概說明之草案普自 105 年 9 月以來供辦理逐七場草案說明會，如現場有簽名，請列出當時各場次男女參與人數及比例。如未登錄性別，可根據性名推測，同時提醒主辦單位覆後應納入性別欄位。 3. 4-1-3 提及人才培訓時，會鼓勵少數性別參與之措施，例如：規劃培訓活動時，考量不同性別之參訓需求，如提供妥適的哺集乳空間；培訓時間避免影響接送年幼子女上下學之時段；培訓地點…等等。建議未來培訓活動簽到紀錄單，除應納入性別欄位外，亦應加註時間(段)及會議場所是否有集哺乳空間。 4. 4-1-3 說明，最後段落「宣傳培訓活動時，納入鼓勵女性參加之文字或圖片，以破除性別刻板印象」建議修改文字如「宣傳培訓活動時，為擴大參與，避免刻板印象，應納入鼓勵多元性別和族群參加之文字或圖片。」原文字特別指出女性，已隱含刻板印象。 5. 往後行政院轄組諮詢委員會或資安會議時，其成員亦應納入性別及族群考量。
（三）參與時機及方式之合宜性	合宜
本人同意恪遵保密義務，未經部會同意不得逕自對外公開所評估之法案。 （簽章，簽名或打字皆可）__吳嘉麗__	

＊ 第一部分「捌、8-1 規範對象」8-1-1 至 8-1-3 皆評定為「否」者，若經程序參與後，11-5「法案與性別議題關聯之程度」評定為「有關」者，則需修正列第一部分「捌、8-1 規範對象」，並補填列「捌、8-2 性別目標、8-3 性別效益」及「玖、評估結果」。

＊ 本表所提專有名詞之定義及參考資料，請詳見「性別影響評估操作指南」（網址：http://www.gec.ey.gov.tw/cp.aspx?n=FC0CD59A5BF00232）。

陸、徵詢及協商程序之附表

重要事項	有無爭議	相關條文	相關機關（構）、團體或人員之主要意見	參採與否及其理由（含國際參考案例）
1. 立法目的事項	□有 ■無	§1	應予清楚定義並在本草案中訂定實際之作法。	1. 關於釐清立法目的：現行版本已調整草案第 1 條，以釐清立法目的。本法立法目的在確保國家安全、維護社會公共利益，促進產業發展則為本法為達成上述目的所採取之方式，為釐清此立法意旨，爰修正第 1 條為「第一條　為積極推動國家資通安全政策，加速建構國家資通安全環境，帶動資通安全產業發展，以確保國家安全、維護社會公共利益，特制定本法」 2. 關於實際做法：草案已就行政院及各機關之權責及受規範之公務與非公務機關之義務進行規定。更細部之作法將於子法或於執行面處理之。
2. 執行資源	□有 ■無	§4 §15V §16III §17III	1. 建議減少例行文書作業、避免重複查核。 2. 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。	1. 目前版本已調整草案第 15 條第 5 項、第 16 條第 3 項、第 17 條第 3 項等條項，將例如矯正、預防報告及矯正、預防計畫整併為矯正計畫，以減少文書作業。 2. 關於避免重複稽核：

				日後執行面將由行政院資安處就資安事項統一作整體之資源調度與協調，並將相關稽核工作整併，以簡化程序及有關機關之人力、資源。 3. 目前草案第 4 條規定，政府應提供相關資源並推動國家資通安全科技之研發；日後於執行面上亦會以此為規劃方向。
3. 行政院及中央目的事業主管機關權責	□有 ■無	§4	1. 建議於草案中規定行政院應籌組諮詢委員會或資安會議，結合不同專業之跨領域代表。 2. 建議實行上應以專責機關為立法對象，並清楚定義專責機關之專業執掌，整清資訊、資安主責單位。	1. 目前實務運作上資安會報中已有資安諮詢會，成員即包括業界及學者專家。 2. 適用本草案之公務機關，除行政院及所屬機關外，尚包含其他中央及地方機關（參考草案第 2 條第 4 款公務機關之定義）。因資安事務具高度重要性，且行政院具有統籌資安事務之資源，亦具有協調各部會之高度，故由行政院負責規劃推動國家資通安全政策等事宜（參考草案第 4 條關於行政院權責規定），並由資安處協助統籌辦理。
4. 本法適用對象	□有 ■無	座談會版§16 II（現行	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，建議應以先以政府為主，再	1. 草案刪除原有之 16II 後，現係以公務機關、關鍵基礎設施、其他公營事業及由公

		版本已刪除此規定)	逐步推廣到關鍵基礎設施，一般民間企業先不要考慮。 2. 境外單位是否適用?	務機關或公營事業捐助成立之財團法人，且其捐助財產合計超過該財團法人之基金總額達行政院所定一定比例者為主要規範對象。關鍵基礎設施提供者之清單將由中央目的事業主管機關評估後提出交行政院核定；至於未來本法規範是否應擴及其他產業，將持續研析，並在符合我國需求及與國際接軌之前提下考量是否納入。 2. 境外單位未必有本法資安維護計畫等義務(須為符合本法定義之公務機關和非公務機關方受規範)，但如為本法公務機關或非公務機關委外的受託者時，仍依本法第 8 條規定受機關監督。
5. 有關關鍵基礎設施及關鍵基礎設施提供者範疇事項	□有 ■無	§2(6)(7)	1. 關鍵基礎設施及關鍵基礎設施提供者之認定	1. 關鍵基礎設施定義為：「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，對公共利益、國民生活、經濟活動、公眾安全或國家安全有重大影響之虞，並經行政院公告者」。 2. 關鍵基礎設施提供者，係指提供關鍵基礎設施之全部或一

				部，並經中央目的事業主管機關提請行政院核定者。由中央目的事業主管機關對其所熟悉管理之業務為指定，並由行政院核定，較為嚴謹。
6. 有關安全維護義務	□有 ■無	§15VI §16IV	1. 草案目前多以制定安全維護計畫為主，無法有效解決資安問題。 2. 建議中央目的事業主管機關可以提供整套的資安維護範本，以讓民間有所遵循。	1. 本法從制度面上要求公務機關及關鍵基礎設施等非公務機關訂定安全維護計畫，乃是為使上開機關得以及時主動以風險管理為考量於其安全維護計畫中反應快速變遷之資安環境，而不至於僅僅遵守明文規定之具體事項。 2. 關於安全維護計畫之範本，草案已有相關規定：第15條第6項及第16條第4項規定，就資通安全維護計畫必要事項等內容，授權由中央目的事業主管機關訂定，以利非公務機關遵循；然非公務機關仍需視自身情況進行風險評鑑與因應，並採取適當之安全維護計畫。日後推動時，資安處亦會提供適當資訊，讓各中央目的事業主管機關參考。
7. 通報應變機制事項	□有 ■無	§17	1. 本草案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	1. 已修正草案第17條第2項，將通報時機調整為「知悉」後，而非「發

			並不知情，等到發現時已是事後是否應調整? 2. 通報作業可否統一規劃，避免須一再通報，並建議依既有管道與機制。	生_後。 2. 草案目前即是依現行機制辦理。例如非公務機關是向中央目的事業主管機關通報。另外在執行面資安處亦已與如調查局進行合作，避免機關須多次通報。且機制上是設計成電子方式通報，應可避免重工問題。
8. 數位證據保全事項	□有 ■無	N/A	1. 證據保全與專業鑑識部分，係為整個安全機制之模型之重要部分，建議應予納入。	1. 評估後未增訂數位證據保全規定。 2. 證據保全為訴訟法之規定，且刑事訴訟法中已有證據保全之規範，無須於本法另為規定。此外，在政府機關部分，「政府機關（構）資安事件數位證據保全標準作業程序」實行已有相當時日，其效果如何，是否為司法機關所採納，仍賴相關單位評估。
9. 委外辦理事項	□有 ■無	§8	1. 辦理評選時，如資通安全成績最高者未必為整體評選成績最高者，建議酌修本草案委外監督規定之文字內容或修訂相關配套措施，以利遵循。 2. 本草案受託者委外監督部分(草案第 8 條)，建議可限縮在受委託範圍；建議委外監督部分	1. 草案第 8 條規定並非要求採購時，僅須以資通安全成績為據，仍應綜合考量各項，惟須考量必要之資通安全維護能力。各機關在評分時，資安應占幾分也不會是一成不變，重要的資訊系統資安評分可能就占比需要重一些。

			應訂定監督標準以利遵循。	2. 公務機關委外的部分：有關資通系統採購的相關事宜，涉及採購法的規範，未來資安處也將持續就提昇資通系統資安能力的部份進行努力，目前的作法是透過服務水準協議的方式進行資安能力的要求，未來也將持續提供相關的指引與方針，供各機關參考。 3. 目前條文解釋上監督亦僅限於與委託範圍相關部分。 4. 未來將於細則提出委外監督相關事項之細部規定。
10. 行政檢查及司法警察、專業人員陪同執行行政檢查事項	□有 ■無	§18	1. 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。 2. 草案未見行政檢查之相關配套行政訴願及救濟程序。	1. 目前草案已刪除行政檢查條文關於司法警察陪同檢查之規定；因此可依行政程序法第19條行政協助之規定處理，為避免重複規定，故刪除之。 2. 人民就國家公權力所為之行政行為本得依法提起訴願、行政訴訟等，故本草案所規範之行政檢查，自得依行政程序法、訴願法、行政訴訟法或其他法律規定提起救濟，無須於草案中另行規定。
11. 獎懲與罰則事項	□有 ■無	§14 §19	1. 建議依比例原則，先令限期改正後再科予罰	1. 已調整草案19條，修訂為先命限期改正，

		§20 §21	緩。（業者） 2. 對非公務機關之罰則輕重或可再討論。 3. 對於公務機關人員之獎懲應注意衡平。 4. 對於非公務機關建議應納入相關的獎勵機制。	屆期未改正按次處罰之規定。至於第21條所處罰者為非公務機關或其相關人員故意違反義務之行為；第20條則考量不依規定通報可能致生更大損害，為免貽誤通報時機，故仍規定先予處罰。 2. 本法所納管之非公務機關以關鍵基礎設施提供者為主並兼及其他具有公共色彩之非公務機關（如公營事業、由公務機關或公營事業捐助財產達一定比例之財團法人），其如發生資安事件之嚴重性較高，故為目前罰則規定。 3. 公務機關獎懲部分會另訂獎懲辦法（子法），訂定時會注意獎懲之平衡與合宜。 4. 對非公務機關獎勵大多透過租稅減免之方式，惟此涉及國家租稅政策，影響重大，且現行已有產業創新條例等法律相關規定，故暫不於本草案中訂定。
12. 有關法規適用與競合	□有 ■無	N/A	1. 建議草案應與其他法規之適用區別、競合關係與協調統一彙整，例如個人資料保護法已規定通知當事人之義務，惟本草案無此規定，日後恐衍生適用性問題。	本草案規定已於工作小組會議中請益過法務部法律事務司，因個人資料保護法與本草案之規範目的及範圍不同，二法律間並無衝突。本草案如經制定公布，未來

				可能與個人資料保護法產生競合之情形，例如非公務機關同時違反本草案與個人資料保護法第27條規定，此時為一行為違反數個行政法上義務規定之問題，依行政罰法規定從重處罰即可。
13. 人才培育事項	□有 ■無	§3	1. 建議各部會建立資安人才培育機制。	未來將研擬與各部會建立資安人才培育機制，同時研擬認證機制。
14. 其他事項	□有 ■無	N/A	1. 本法有違憲、圖利資安業者之虞，是否有訂定之必要。 2. 如屬國安層面之攻擊建議放入國土安全法較為合適。 3. 部分文字應予調修。	1. 本法旨在從資安面向保障國家安全與人民福祉，至於產業發展則為附帶影響，且法律環境的提升，間接受益者並不限於特定廠商，不能因為本法可能促進產業發展，即不為之。 2. 本法旨在要求受規範之公務機關及非公務機關，從制度面採取訂定安全維護計畫並通報相關事件之資通安全維護與因應方式，此並不妨礙日後於國安法規中，就相關事項另為特殊要求；且執行上只要公務機關及非公務機關將其他法律之要求亦納入安全維護計畫及通報程序一併處理即可。 3. 會後已透過會議，就本草案各條文文字，

	再予檢視、調整。部分用語如「重大資安事件」會於子法中訂定。

註：為茲簡明，「相關條文」欄位中，各條、項、款、目等，分以下列方式表述：條→§（條號以阿拉伯數字表述）、項→Ⅰ（羅馬符號）、款→⑴（括弧內置阿拉伯數字）、目→㈠（圓圈內置阿拉伯數字），目以下則以「之○（阿拉伯數字）」表述。

三：立法院法制局法案性別與人權影響評估檢視表

立法院法制局法案性別與人權影響評估檢視表

105.3.23

壹、法案名稱	**資通安全管理法草案**
貳、主管機關	**行政院**

參、法案內容涉及領域：	**勾選（可複選）**
3-1 權力、決策、影響力領域	
3-2 就業、經濟、福利領域	
3-3 人口、婚姻、家庭領域	
3-4 教育、文化、媒體領域	
3-5 人身安全、司法領域	
3-6 健康、醫療、照顧領域	
3-7 環境、能源、科技領域	V
3-8 其他（勾選「其他」欄位者，請簡述法案涉及領域）	

肆、主管機關法案及性別影響評估檢視表檢視結果

檢視項目	內容	檢視結果
4-1 提案機關之性別影響評估之檢視	4-1-1 檢視表是否檢附到立法院	□是 □否 ■其他（請說明）非行政院所屬機關，無此表
	4-1-2 檢視表是否依程序填報	□是 □否 ■其他（請說明）無檢視表
	4-1-3 是否為相關之性別統計及性別分析	□是 □否 ■其他（請說明）無檢視表
4-2 與本法案相關之配套法案及機關	4-2-1 是否因性別觀點而需配套修正之相關法案	□是，法案名稱： ■否 □其他（請說明）
	4-2-2 是否因性別觀點而需協力之機關	□是，協力機關： ■否 □其他（請說明）

伍、機關提案之性別議題相關性

5-1 規範對象

項　目	檢視結果	備　註

5-1-1 法案內容是否以特定性別、性傾向或性別認同者為規範對象	□是 ■否 □其他（請說明）	例如規範對象以男性或女性為主，或以同性戀、異性戀或雙性戀為主，或個人自認屬於男性或女性者，是否涉及本法案條文。
5-1-2 法案內容未區別對象，但是否其執行方式將因性別、性傾向或性別認同不同而有差異	□是 ■否 □其他（請說明）	規範對象雖無區別，但因性別、性傾向或性別認同之本質差異，而有不同執行方式者，是否涉及本法案條文。
5-1-3 法案內容所規範對象及執行方式無差異，但是否對於不同性別、性傾向或性別認同者將產生不同結果	□是 ■否 □其他（請說明）	規範對象及執行方式雖無差異，惟其結果乃因性別、性傾向或性別認同而有不同者，是否涉及本法案條文。

5-2 性別目標

項　目	檢視結果	備　註
5-2-1 法案內容是否採取積極作為，去除不必要差別待遇，或促進實質平等；營造平等環境，預防及消除性別歧視目標	□是 ■否 □其他（請說明）	一、基於憲法平等權之規定，採行一定方式去除現行法規及其執行所造成之差別待遇，或提供較為弱勢之一方必要之協助，以促進其實質地位之平等。 二、消除或打破性別刻板印象與性別隔離，以消弭因社會文化面向所形成之差異，或提供不同性別、性傾向或性別認同者平等機會獲取社會資源，提升其參與社會及公共事務之機會。 三、本法案是否須採更積極作為以符合預防及消除性別歧視目標。

5-3 性別效益

項　目	檢視結果	備　註
5-3-1 法案是否對於消弭性別歧視、促進性別平等有積極、正面綜效	□是 ■否 □其他（請說明）	主管機關所列性別效益，是否有助消弭性別歧視、促進性別平等有積極正面綜效。
5-3-2 法案是否符合憲法、國際規範(包括消除對婦女一切形式歧視公約 CEDAW)、性別平等政策綱領等要求	■是 □否 □其他（請說明）	依消除對婦女一切形式歧視公約施行法，主管機關應檢視法案是否符合公約(CEDAW)規定及其一般性建議，請再檢核本法案內容是否合宜。

陸、機關提案對人權之影響		
6-1 對人權之影響		
項　目	檢視結果	備　註
6-1-1 法案是否符合憲法有關人民權利之規定	■是 □否 □其他（請說明）	請檢視法案是否符合憲法有關人民權利之規定及司法院解釋。
6-1-2 法案是否符合公民與政治權利國際公約	■是 □否 □其他（請說明）	依公民與政治權利國際公約及經濟社會文化權利國際公約施行法，請檢視法案是否符合公約規定及聯合國人權事務委員會之一般性意見，以積極促進各項人權之實現。
6-1-3 法案是否符合經濟社會文化權利國際公約	■是 □否 □其他（請說明）	依公民與政治權利國際公約及經濟社會文化權利國際公約施行法，請檢視法案是否符合公約規定及聯合國經濟社會文化權利委員會之一般性意見，以積極促進各項人權之實現。

柒、性別與人權影響評估結果：

依據參加本法案評估報告草案座談會或書面審查之專家學者意見，綜合說明本法案之性別與人權影響評估意見。

7-1 專家學者意見綜合說明	1、本次「資通安全管理法草案」部分條文修正的主要目的在於：「制定一部協助公務機關及受規範之非公務機關，認知自身資通安全風險並逐步提升自身資通安全能量之專法，遂成現階段建構、提升資通安全環境最有效率之規範面政策選擇。」 2、該草案內容經性別影響評估之檢視結果顯示：本法案之修正條文內容規範對象並未以特定性別、性傾向或性別認同者為規範對象。其次，執行方式也未因性別、性傾向或性別認同之不同而有差異。正因為對於性別對象與執行方式並無區別，所以，就不會因為不同性別、性傾向或性別認同者而可能產生不同之結果。 3、在人權影響評估部分，經初步檢視結果顯示：本法案之修

	正條文尚能符合我國憲法、國際規範、性別平等政策綱領等要求，也符合我國憲法有關人民權利之規定，以及聯合國人權兩公約：「公民與政治權利國際公約」和「經濟社會文化權利國際公約」中有關人民權利保障之基本精神。 簽名：葉肅科 **(必填)** 日期：106 年 6 月 27 日 **(必填)**	
7-2 參採情形	7-2-1 說明採納意見後之報告調整	
	7-2-2 說明未參採之理由或替代規劃	經評估本評估報告內容未涉及性別議題，草案內容亦符合憲法、兩公約施行法及 CEDAW 施行法等有關人民權利保障之規範，爰報告無須調整。