立法院議案關係文書

院總第1570號　　委員提案第 19694 號

案由：本院委員陳亭妃、陳歐珀、蘇震清等23人，有鑑於全球化、資訊化時代來臨，政府及企業大量使用網際網路進行線上服務，且許多重要關鍵基礎設施也開始仰賴網路線上管理後，來自有心人士或國家，以及網際網路的駭客，會盜用國人身分、侵入公家與個人之電子郵箱，試圖破壞資訊網路、金融機構及資訊管理系統，以竊取我國政府或企業的機密。而我國公部門，雖有資通安全推動單位與相關遵行法令，惟若能進一步賦予各機關資通安全維護義務的法源，將更能提昇我國資通安全能量。另外，在私部門方面，雖有資通安全相關法令，但其訂定目的大相逕庭，故須對整體資通環境之法規予以建立。此外，各國越來越關注全球駭客竊取智慧財產、商業機密，以及重要國家安全與外交、國防軍事資料，應視為國家安全與國人生命財產安全的一環。基此，特擬具「資通安全管理法草案」之專法，俾利強化我國資通安全，並降低資通安全之風險。是否有當？敬請公決。

提案人：	陳亭妃	陳歐珀	蘇震清		
連署人：	陳賴素美	許智傑	柯建銘	鍾孔炤	黃秀芳
	陳曼麗	羅致政	黃國書	施義芳	洪宗熠
	陳素月	賴瑞隆	蔡易餘	鍾佳濱	何欣純
	姚文智	李俊俋	陳明文	張廖萬堅	陳其邁

資通安全管理法草案

條文	說明
第一章　總則	章名
第一條　為積極推動國家資通安全政策，強化我國資通安全，並降低資通安全之風險，以確保國家安全、維護國人之生命權及財產權，並提升資通安全產業發展，特制定本法。	一、全球化、資訊化時代來臨，政府及企業大量使用網際網路進行線上服務，且許多重要關鍵基礎設施也開始仰賴網路線上管理後，來自網際網路的駭客，會盜用民眾身分，侵入個人電子郵箱，試圖破壞資訊網路、金融機構及資訊管理系統，以竊取他國政府或企業的機密。世界正面臨著快速增長的網路安全威脅，各國越來越關注全球駭客持續入侵、竊取智慧財產、商業機密以及國防軍事資料，對經濟和國安造成威脅。我國資訊科技發展快速，受到網路攻擊的危機迫切，網路安全問題已是國家安全的重要議題，實有必要立法規定。 二、鑒於數位及其他資訊科技應用普及，資通科技的蓬勃發展，資通安全風險大幅增加，而我國公部門，雖有資通安全推動單位與相關遵行法令，惟若能進一步賦予各機關資通安全維護義務的法源，將更能提昇我國資通安全能量。 三、為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，以確保國家安全、維護國人之生命權及財產權，並提升資通安全產業發展。
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、修改、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、地方機關或行政法人。 五、非公務機關：指公務機關以外之自然人、公營事業機構、其他法人或團體。 六、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、中央與地方機關、高科技園區等實體或虛擬資產、系統或網路，其功能一旦停止運作或效能降低，將使國人生活、經濟活動、公眾安全或國家安全有重大影響。	一、本法用詞定義之規定。 二、參考美國國家標準技術研究所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，針對資通系統、資通安全等用詞定義進行規定。 三、定義公務機關與非公務機關參考個人資料保護法之規定內容，公務機關包含中央、地方機關或行政法人，例如總統府、行政院、立法院、司法院、考試院、監察院、縣（市）政府、公立教育機構或醫療機構等，均屬之；非公務機關則指公務機關以外之自然人、公營事業機構等法人或團體，例如私立教育機構及醫療機構等，均屬之。 四、參考美國「關鍵基礎設施」定義、日本「網路資訊安全基本法」、韓國「情報通信基礎保護法」來定義「關鍵基礎設施」。 五、各運作的關鍵基礎設施之非公務機關於各該類關鍵基礎設施中之屬性及重要性有所

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，並經中央目的事業主管機關指定之非公務機關。	不同，所以由中央目的事業主管機關指定其中具重要性或亟具關鍵者納入規範對象。
第三條　為提升資通安全，政府應提供資源，整合民間力量，提升全民資通安全意識，促進資通安全產業發展，進而落實於公、私部門，應推動下列事項： 一、資通安全專業人才之培育。 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、資通安全軟體、設備技術規範、相關服務及審驗機制之發展及推動。	一、基於確保資訊及網路安全所需，先進國家無不加強相關防護作為，立法要求政府機關與相關的企業加強資訊分享，共同建立資訊及網路安全防護的執行架構，美國及日本等國家甚至成立網軍以鞏固資安防線。 二、我國面臨網路犯罪與駭客入侵癱瘓政府機關網站案件日增。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、軟體、設備、專業人才等。是以，政府應與民間共同提升全民資通安全意識，推動資通安全產業之發展，以利先進資通安全技術、軟體、設備、專業人才等之發展。 三、在外國立法例上，參考日本網路資訊安全基本法之人才之確保等規定；韓國情報通信基礎保護法之技術開發與人力養成等規定定之。
第四條　行政院應擘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諸多相關事宜。	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，由行政院主動規劃相關措施，以落實資通安全政策。
第五條　行政院得委任或委託其他公務機關、法人或團體，辦理資通安全科技研發、國際資安政策研析與國際交流合作、公務機關資通安全整體防護之執行及其他相關事務。	行政院擘劃並推動資通安全政策、發展資通安全科技與國際交流合作，並負責資通安全防護相關工作之監督與執行，於必要時得將部分事務委任或委託其他公務機關、法人或團體辦理。
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；其適用對象、分級基準、等級變更申請、義務內容、專職人員之設置及其他相關事項之辦法，由行政院定之。 行政院應查核所屬或監督之公務機關及適用前項辦法之非公務機關之資通安全維護情形。 公務機關及非公務機關受前項之查核，經發現其資通安全有缺失或待改善者，應完成矯正、預防報告或提出矯正、預防計畫，送交上級機關、監督機關及中央目的事業主管機關。	一、考量公務機關與非公務機關之規模與業務性質不一，故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，宜因機關裁撤、組織更改、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，爰規定行政院應訂定資通安全責任等級之分級辦法，就辦法之適用對象、分級之標準、義務內容及專職人員之設置、等級變更申請及其他相關事項加以規定。 二、行政院應考量資通安全責任等級分級辦法所適用對象之責任等級、其過往資安維護狀況及其他相關情形，查核上述適用對象中之非公務機關及行政院所屬或監督之各級公務機關之資通安全維護情形，受查核機關如有缺失或宜改善事項應完成矯正、預防或提出矯正、預防計畫，並將相關報告送交上級或監督機關及中央目的事業主管機關，由各該機關續行確認矯正、預防與改善之狀況。
第七條　行政院應建立資通安全情資分享機	為增進與改善我國境內面對資通安全威脅與風

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。	險的應變能力與策略擬定，應建立相關資通安全情資分享機制，並須就情資之分析、整合、情資分享之內容、程序及方法及其他相關事項訂定辦法，以資遵循。
第八條　公務機關或非公務機關，應考量國家安全及本法適用範圍內之前提下，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，並定期就受託者之資通安全維護為監督。	公務機關或非公務機關委外辦理資通系統建置、維運或資通服務之提供時，應考量國家安全及本法適用範圍內，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，以確保國人安全及權利、公共利益等。
第二章　公務機關資通安全管理	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。	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，總統府、行政院、立法院、司法院、考試院、監察院、直轄市、縣（市）政府及直轄市議會、縣（市）議會及其他各級中央或地方機關及行政法人，應考量其所屬之資通安全責任等級、其所保有或處理之資訊種類、數量及性質、資通系統之規模及性質等條件，衡酌機關資源之合理分配，配置人員、必要資源，並依循上級或監督機關之相關資安規則，訂定、修正及實施資通安全維護計畫。
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工作與事項。	為確保有效推動資通安全維護事項，公務機關應設置資通安全長並由其成立相關推動組織與督導推動相關工作。爰參考美國2014年聯邦資訊安全現代化法之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定之。
第十一條　公務機關應於年度終了後，就其資通安全維護計畫之實施情形，向上級及監督機關提出報告；無上級機關或監督機關者，其報告應送交行政院。	一、公務機關應每年提出該年度之資通安全維護計畫實施情形報告，以確認自身實施資通安全計畫之成效。又為利行政院提供必要協助，或使上級及監督機關了解所屬或監督機關之年度資通安全維護情形，故規定總統府、立法院、司法院、考試院、監察院、直轄市政府、直轄市議會、縣（市）政府及縣（市）議會等無上級機關或監督機關之公務機關，應將資通安全維護計畫實施情形報告送行政院，其他公務機關則應將報告提交予其上級及監督機關。 二、參考日本網路資訊安全基本法之規定，促進地方公共團體確保網路資訊安全之相關事項，及相關行政機關之首長，應適時地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。
第十二條　公務機關應查核其所屬及監督公務	一、總統府、立法院、司法院、考試院、監察

機關之資通安全維護計畫實施情形。 受查核機關之資通安全維護計畫實施有缺失或待改善者，應完成矯正、預防報告或提出矯正、預防計畫，送交上級及監督機關。	院、直轄市政府、縣（市）政府等各級中央與地方機關應對於其所屬或監督之各級公務機關資通安全維護計畫之實施，依其所屬或監督機關之層級、業務及其他相關情形，就查核之標準、頻率、內容與方法訂定相關行政規則，並進行查核，以了解資通安全維護計畫之落實情形。 二、受查核機關如有缺失，應向上級或監督機關提出缺失之矯正、預防情形或計畫，以確保資通安全維護計畫之落實，與政府資通安全維護的強度。
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。 公務機關發生資通安全事件時，除應通報上級及監督機關外，並應通報行政院；無上級機關或監督機關者，應通報行政院。 公務機關應向上級及監督機關提出資通安全事件調查、處理及矯正、預防情形或計畫之報告，並送交行政院；無上級機關或監督機關者，其報告應送交行政院。 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。	一、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）政府等各級中央與地方機關及行政法人為即時掌控資通安全事件，並有效降低其所造成之損害，應建立資通安全事件之通報、應變機制。 二、參考日本網路資訊安全基本法之因應對我國安全有造成重大影響之虞事件之處理方針與政策精神，規定如有發生重大資通安全事件，總統府、立法院、司法院、考試院、監察院、直轄市政府、縣（市）政府，及直轄市議會、縣（市）議會應向行政院為通報，其他各級公務機關應向其上級及監督機關，以及行政院通報；並應續採取矯正預防措施，以及送交報告或矯正、預防計畫。 三、本條第四項授權行政院就第一項至第三項之通報、應變機制及其他相關事項，訂定相關辦法。
第十四條　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。 公務機關所屬人員未遵守相關資通安全義務，致國家或社會受有重大損害時，除依法追訴行為人相關行政責任及法律責任外，並應追究行為人之服務機關資通安全長及相關人員之行政責任及法律責任。 前二項獎懲基準及其他相關事項之辦法，由行政院定之。	為加強公務機關所屬人員對於資通安全工作之重視與投入，爰對相關獎懲機制進行規範，以提升我國公務機關相關人員責任感及對資通安全重視。
第三章　非公務機關資通安全管理	章名
第十五條　為確保國民生活、經濟活動、公眾及國家之安全，中央目的事業主管機關應指定關鍵基礎設施提供者，並將其清單報請行政院核定之。 關鍵基礎設施提供者應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就其資通安全維護計畫之實施情形，向中央目的事業主管機關提出報告。	一、對於關鍵基礎設施提供者之資通安全保護，乃現今國際針對資通安全保護所重視之議題，爰參考歐盟2016年「網絡與資訊系統安全指令」關於關鍵服務營運商清單、關於關鍵服務營運商用以提供關鍵服務的網路與資訊系統，如有影響其安全的事件，關鍵服務營運商須採取適當措施，預防及最小化事件的影響，以確保服務的持續性、美國關鍵基礎設施保護計劃及有關改善關鍵基礎設施網路安全之規定、日本網路資訊安全基本法之重要社會基礎業者之

中央目的事業主管機關應查核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維護計畫實施有缺失或待改善者，應完成矯正、預防報告或提出矯正、預防計畫，送交中央目的事業主管機關。 第二項至第五項之資通安全維護計畫必要事項、實施報告之提出、查核之頻率、內容與方法、矯正、預防報告或計畫之提出及其他應遵行事項辦法，由中央目的事業主管機關定之。	職責及韓國情報通信基礎保護法中央行政機關長官有權指定主要資訊通信基礎設施以及主要資訊通信基礎設施保護措施等立法例，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重大公共利益及人民之生命、財產安全，故應制定、修正及實施資通安全維護計畫。 三、為使中央目的事業主管機關掌握關鍵基礎設施提供者之資通安全維護計畫實施狀況，關鍵基礎設施提供者應定期向中央目的事業主管機關提出資通安全實施報告，以利中央目的事業主管機關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，中央目的事業主管機關應對關鍵基礎設施提供者進行查核。 五、資通安全維護計畫必要事項、資通安全維護計畫實施報告提出、查核之頻率、內容與方法、矯正、預防報告或計畫之提出、及其他應遵行事項之辦法，授權由中央目的事業主管機關訂定。
第十六條　除前條情形外，適用第六條第一項辦法之非公務機關，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得視公共利益、保護人民生命及財產安全之需要，指定前項以外之非公務機關，就其所提供特定類型或性質之產品或服務，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前二項非公務機關，提出資通安全維護計畫實施情形之報告。 中央目的事業主管機關得查核第一項及第二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，應限期要求受查核之非公務機關完成矯正、預防報告或提出矯正、預防計畫。 前四項之資通安全維護計畫必要事項、實施報告之提出、查核之頻率、內容與方法、矯正、預防報告或計畫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定之。	一、非公務機關如屬第五條之資通安全責任等級分級辦法之適用對象，或如其所提供之特定產品或服務經認定與公共利益或與保護人民生命、財產安全相關且有必要而受指定時，縱其非關鍵基礎設施提供者，仍應負相當之資通安全責任，而須制定安全維護計畫並提交計畫實施情形之報告，爰參考日本網路資訊安全基本法，賦予重要社會基礎業者配合政府資安政策之協力義務；另參考歐盟2016年「網絡與資訊系統安全指令」，在關鍵基礎設施提供者以外，另針對數位服務提供商之安全與事件通知進行規定，爰訂定本條，俾利中央目的事業主管機關為公共利益、保護人民生命、財產安全，而認為必要時，仍得指定非公務機關就其所提供之特定類型或性質之產品或服務，制定、修正及實施資通安全維護計畫並提出實施報告與進行查核。 二、有鑑於各行業均有其目的事業主管機關，而資通安全維護與該事業之經營關係密切，宜由原各該中央目的事業主管機關一併監督管理與其業務相關之資通安全維護事項，故本法對於非公務機關資通安全維護之指導、監督、管理及查核，採分散式管理，由各非公務機關之中央目的事業主管機關執行。 三、資通安全維護計畫必要事項、資通安全維護計畫實施報告提出、查核之頻率、內容與方法、矯正、預防報告或計畫之提出、及其他應遵行事項之辦法，授權由中央目

	的事業主管機關訂定。
第十七條　前二條之非公務機關為因應資通安全事件，應訂定通報及應變機制。 前項之非公務機關於發生資通安全事件時，應向中央目的事業主管機關通報。 第一項之非公務機關，應向中央目的事業主管機關提出資通安全事件調查、處理及矯正、預防情形或矯正、預防計畫之報告；如為重大資通安全事件者，其報告並應送交行政院。 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。 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。	一、按受本法規範之非公務機關如發生資通系統遭受破壞，或不當使用等資通安全事件，為使中央目的事業主管機關及行政院即時掌握情況，以協助與監督受本法規範之非公務機關進行緊急應變處置，並在最短時間內回復正常運作，自應以適當方式通報中央目的事業主管機關及行政院。本條參考歐盟2016年「網絡與資訊系統安全指令」之事件通知規定；日本網路資訊安全基本法之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之金融、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、分析中心以作為發生侵害事故時之即時警報與分析體系等規定而訂立。 二、受本法規範之非公務機關為落實資通安全事件通報之要求，自應制定資通安全事件通報機制與相關應變措施，並於事件發生時通報中央目的事業主管機關；受本法規範之非公務機關於事故發生後，亦應提出事件調查、處理及矯正、預防情形或矯正、預防計畫之報告。 三、第一至三項通報、應變機制之必要事項、通報內容、報告提出與其他應遵行事項，宜有相關辦法以為依循，故授權行政院訂定之。 四、於資通安全事件情節重大，可能影響多數人民之生命、身體或財產利益安全時，行政院得會同中央目的事業主管機關知悉後，介入協助處理，並得公告必要之內容與因應之方法，以供民眾防範、避免損害之擴大。
第十八條　中央目的事業主管機關因查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時，應派員攜帶執行職務證明文件，進入第十五條及第十六條之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。 中央目的事業主管機關為前項檢查時，得率同司法警察人員、資訊、電信或法律等專業人員共同為之。 參與檢查之所有人員，對於因檢查而知悉之他人應秘密之資訊，負保密義務。	一、為落實資通安全之維護，應賦予監督機關有命令、檢查及處分權，並參考日本網路資訊安全基本法之政府為促進民間業者採取自發性的措施得採取必要措施。 二、為取締犯罪以及防止傷害之擴大得採取必要措施之規定，爰訂定第一項，規定中央目的事業主管機關必要時，得派員攜帶執行職務證明文件，進入第十五、十六條非公務機關檢查或要求說明、提供相關證明資料，以強化監督機關之權責。 三、檢查資訊系統如未具有相當專業知識，勢必無法達成檢查目的，爰規定檢查機關得率同司法警察人員、資訊、電信或法律等專業人員共同進行檢查。 四、第三項明定因檢查而知悉他人資料者，應負保密義務，不得洩漏。
第四章　罰則	章名
第十九條　非公務機關有下列情形之一者，由	一、本條為對非公務機關未訂定、修正、實施

中央目的事業主管機關處新臺幣五十萬元以上三百萬元以下罰鍰，並令限期改正；屆期未改正者，按次處罰之： 一、違反第十五條第二項規定，未確實訂定、修正或實施資通安全維護計畫。 二、違反第十六條第一項或第二項規定，未確實訂定、修正或實施資通安全維護計畫。	資通安全維護計畫或訂定、修正、實施未確實之罰則規定。 二、非公務機關依第十五條第二項、第十六條第一項及第二項，應訂定、修正、實施資通安全維護計畫，如未依規定訂定、修正或實施，或訂定、修正、實施未確實，應由中央目的事業主管機關處以罰鍰，並令限期改正；屆期未改正者，按次處罰之。 三、參考歐盟2016年「網絡與資訊系統安全指令」之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訂定。
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者，由中央目的事業主管機關處新臺幣三十萬元以上二百萬元以下罰鍰，並令限期改正；屆期未改正者，按次處罰之。	一、本條為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罰則規定。 二、非公務機關如發生資通安全事件，應依本法相關規定進行通報；如未依規定通報，應由中央目的事業主管機關處以罰鍰，並令限期改正；屆期未改正者，按次處罰之。 三、參考歐盟2016年「網絡與資訊系統安全指令」之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訂定。
第二十一條　非公務機關有下列情形之一者，由中央目的事業主管機關處新臺幣六萬元以上六十萬元以下罰鍰，並令限期改正；屆期未改正者，按次處罰之： 一、未依第十五條第三項或第十六條第三項規定，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之報告。 二、未依第十五條第五項或第十六條第四項規定，完成矯正、預防報告或提出矯正、預防計畫送交中央目的事業主管機關。 三、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。 四、違反第十七條第三項規定，未向中央目的事業主管機關提出資通安全事件之調查、處理及矯正、預防報告或計畫，或重大資通安全事件之相關報告或計畫未送交行政院。	一、本條為對非公務機關未依本法相關規定，提出資通安全維護計畫實施情形之報告、送交中央目的事業主管機關矯正、預防報告或計畫、訂定資通安全事件之通報及應變機制；或未依規定向中央目的事業主管機關或行政院提出資通安全事件之調查、處理及矯正、預防報告或計畫之罰則規定。非公務機關如有上述情形，應由中央目的事業主管機關處以罰鍰，並令限期改正；屆期未改正者，按次處罰之。 二、參考歐盟2016年「網絡與資訊系統安全指令」之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訂定。
第二十二條　非公務機關無正當理由違反第十八條第二項規定者，由中央目的事業主管機關處新臺幣四萬元以上四十萬元以下罰鍰。	一、本條為對非公務機關無正當理由妨礙、規避或拒絕行政檢查之罰則規定。 二、非公務機關無正當理由違反第十八條第二項規定者，由中央目的事業主管機關處以罰鍰。 三、參考歐盟2016年之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訂定。
第五章　附則	章名
第二十三條　本法施行細則，由行政院定之。	本條授權行政院訂定施行細則。
第二十四條　本法施行日期，由行政院定之。	本條授權行政院訂定施行日期。